Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Jallé H. Dafa (SBN 290637)
jdafa@lchb.com
Nabila Abdallah (SBN 347764)
nabdallah@lchb.com
LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Facsimile: 415.956.1008

Attorney for Plaintiffs and the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

Michael Katz-Lacabe and Dr. Jennifer Golbeck, on behalf of themselves and all others similarly situated, Plaintiffs, vs. ORACLE AMERICA, INC., a corporation organized under the laws of the State of Delaware, Defendant.	Case No. 3:22-cv-04792-RS **FIRST AMENDED CLASS ACTION COMPLAINT** **CLASS ACTION** **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

I. INTRODUCTION

1. This amended complaint sets forth how the regularly conducted business practices of defendant Oracle America, Inc. ("Oracle") amount to a deliberate and purposeful surveillance of the general population via their digital and online existence. In the course of functioning as a worldwide data broker, Oracle has created a network that tracks in real time and records indefinitely the personal information of hundreds of millions of people. Oracle sells this detailed personal information to third parties, either directly, or through its "ID Graph" and other related products and services derived from this data. The proposed Classes herein lack a direct relationship with Oracle and have no reasonable or practical basis upon which they could legally consent to Oracle's surveillance.

2. The named Plaintiff class representatives are informed and concerned citizens who believe that the unregulated worldwide data marketplace abrogates the privacy and autonomy of the people and threatens core principles essential for democratic self-rule. Plaintiffs bring this action to enforce their fundamental right to privacy, seek redress and compensation for the financial, dignitary, reputational, and relational harms Oracle has caused, and obtain a ruling that Oracle's conduct is unlawful and therefore must stop. The law, as alleged below, entitles Plaintiffs and the proposed Classes to these remedies.

II. THE PARTIES

3. Plaintiff Michael Katz-Lacabe resides in San Leandro, California. Mr. Katz-Lacabe is a privacy rights activist. He is the founder of the Center for Human Rights and Privacy, a project dedicated to the promotion of human rights and privacy in the United States, focusing on the use of surveillance technologies by local police and other government agencies.[1] Mr. Katz-Lacabe is also an active member of Oakland Privacy, a grassroots citizens' coalition that "works regionally to defend the right to privacy and enhance public transparency and oversight regarding the use of surveillance techniques and equipment."[2] Mr. Katz-Lacabe has been frequently cited by

[1] *About CEHRP*, The Center for Human Rights and Privacy (2014), https://www.cehrp.org/about-cehrp/ [https://perma.cc/9T3N-ZH5W].

[2] *About*, Oakland Privacy (2022), https://oaklandprivacy.org/about/ [https://perma.cc/N8VH-5TCH].

reporters for his privacy work related to the use of license plate readers by local police,[3] which has been referenced by advocacy organizations in their California Supreme Court *Amicus Curiae* briefs.[4]

4. Mr. Katz-Lacabe, like most members of modern society, must use the Internet to conduct routine affairs of daily life. On May 4, 2022, despite taking significant steps to maintain his online and offline privacy, Mr. Katz-Lacabe received an "Offline Access Request Response Report" ("OARRR") from Oracle indicating Oracle had tracked, compiled, and analyzed his web browsing, geolocation, brick-and-mortar purchase, and other activity and thereby created an electronic profile on him, attached hereto as Exhibit A. On information and belief, Oracle continues to track Mr. Katz-Lacabe's internet and offline activity, enrich the profile of him as described below, and make his personal information available to third parties without his consent. On information and belief, Mr. Katz-Lacabe has visited websites where his electronic communications were intercepted by the use of Oracle JavaScript code, as described below.

5. The full scope and extent of Oracle's tracking and compiling of Mr. Katz-Lacabe's internet and offline activity and personal data resides with Oracle itself, is not fully disclosed by Oracle, and therefore must be determined through discovery from Oracle. Based on information known at this time, Mr. Katz-Lacabe alleges as follows.

6. Oracle has tracked Mr. Katz-Lacabe's activity on at least hundreds of websites. Mr. Katz-Lacabe has searched for and viewed articles related to political and personal financial issues on numerous websites. Oracle tracking mechanisms, including "cookies," "pixels," and/or

[3] Cyrus Farivar, *Op-Ed: Technology TurnsOour Cities into Spies for ICE, Whether We Like it or Not*, Los Angeles Times (May 2, 2018, 4:15 AM), https://www.latimes.com/opinion/op-ed/la-oe-farivar-surveillance-tech-20180502-story.html [https://perma.cc/89AL-WMA4]*;* Cyrus Farivar, *California cities, counties have spent $65M on spy tech in past decade*, Ars Technica (Nov. 12, 2014, 6:45 AM), https://arstechnica.com/tech-policy/2014/11/california-cities-counties-have-spent-65m-on-spy-tech-in-past-decade/ [https://perma.cc/NA4Z-MRV9]; Andy Greenberg & Ryan Mac, *How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut*, Forbes (Aug.14, 2013, 10:10 AM), https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/?sh=6b9236727785[https://perma.cc/25ZT-BBL6].

[4] *Application for Leave to File Amicus Curiae Brief and Amicus Curiae Brief of Electronic Privacy Information Center (EPIC) in Support of Petitioners*, Supreme Court of the State of California (May 17, 2016), https://www.courts.ca.gov/documents/15-s227106-ac-elec-privacy-info-ctr-051716.pdf [https://perma.cc/PBK6-LDFJ].

javascript code, as described below at paragraphs 41-59, were present on those websites, including, on information and belief, at the time Mr. Katz-Lacabe accessed them. Those tracking mechanisms transmitted to Oracle the URL data coupled with unique identifiers that Oracle used to associate that browsing history with other data compiled into a data profile about him. On information and belief, the bk-coretag javascript code was present on a subset of websites at the time Mr. Katz-Lacabe read those articles, and that code transmitted to Oracle the URLs for the specific articles and web pages he was reading to Oracle, and also transmitted information he entered into fields on these websites, including but not limited to search terms, as well as add-to-cart actions, and other communications with websites. Oracle maintains a data profile concerning Mr. Katz-Lacabe, which Oracle provides direct access or indirect access (e.g., via products or services derived from the profile) to unknown third parties. On information and belief, Oracle engaged in this conduct throughout the class period. The websites visited by Mr. Katz-Lacabe where Oracle tracking mechanisms have been detected include but are not limited to:

a. abcnews.com

b. citi.com

c. fivethirtyeight.com

d. govdelivery.com

e. ktla.com

f. nasdaq.com

g. nytimes.com

7. Oracle partnered with a company called PlaceIQ to obtain, compile, and analyze hundreds of physical locations Mr. Katz-Lacabe had traveled to, and then made that data, or information derived from that data (such as “segments” described at paragraphs 57, 64, and 74-76 below), via products or services derived from that profile available to unknown third parties through its Data Marketeplace. According to a press release, “PlaceIQ, the company building a new model of consumer behavior by connecting physical and digital activities across time, space, and mobile devices,” made “PlaceIQ audience data available through Oracle Data Cloud’s BlueKai Marketplace,” and “[t]his integration gives Oracle Data Cloud users convenient access to

PlaceIQ's rich consumer audiences, built from real world movement data and observations."[5] Oracle thus provided unknown third parties with "convenient access" to Mr. Katz-Lacabe's "real world movement data." Mr. Katz-Lacabe was neither aware of nor consented to this conduct. The Center for Digital Democracy has urged the FTC to open an inquiry into Place IQ's practices, as these practices "may lead to new forms of discrimination, as consumers are treated differently based on race, ethnicity, income, etc."[6] Through PlaceIQ, Oracle tracked Mr. Katz-Lacabe's activity at hundreds of specific locations, including:

a. retail locations;

b. restaurants;

c. gas stations;

d. banks—including the specific type of bank and branch, thereby revealing which banks Katz-Lacabe does business with; and

8. Oracle obtained, compiled, and analyzed information about hundreds of Mr. Katz-Lacabe credit card purchases, and then made that data or information derived from that data (such as "segments" described at paragraphs 57, 64, and 74-76 below), via products or services derived from that profile available to third parties through its Data Marketplace. On information and belief, Oracle obtained, and continues to maintain in its systems, information about his credit card purchases, including reflecting specific spending habits and preferences, as well as specific purchase amounts and even SKUs for specific products. For instance, the OARRR states "Oracle Data Cloud collected purchase-related retail data associated with your profile, indicating that you spent the following amounts at retail businesses in the last 12 months," and lists a specific purchase for a specific product, including the SKU identifying the product, as well the price Mr.

[5] *PlaceIQ Data Now Available Through Oracle Data Cloud's BlueKai Marketplace*, PlaceIQ (July 13, 2016), https://www.placeiq.com/2016/07/placeiq-data-now-available-through-oracle-data-clouds-bluekai-marketplace/ [https://perma.cc/22T8-MVGZ]

[6] U.S. PIRG and the Center for Digital Democracy, Protecting Consumer Privacy and Welfare in the Era of "E-scores," Real-time Big Data "Lead-Generation" Practices and other Scoring/Profile Applications. https://www.democraticmedia.org/sites/default/files/AltScoringCommentsFTC18March14PIRG%26CDD_0.pdf[https://perma.cc/2R97-F7WK].

Katz-Lacabe paid for that product. Mr. Katz-Lacabe was neither aware of nor consented to this conduct.

9. The OARRR also demonstrates that Oracle obtained, compiled, and analyzed sensitive information about Mr. Katz-Lacabe's finances and credit, including information about his ability to pay a mortgage, his creditworthiness, and the risks he presents to potential creditors.

10. Oracle associated the above information with a profile through its ID Graph, as described below, that contained detailed demographic information about him, as well as his name, email addresses, physical address, and phone numbers. As such, a person in possession of any of these identifiers, along with access to Oracle's dossier on him, could learn highly detailed, sensitive information about him.

11. Plaintiff Dr. Jennifer Golbeck resides in Sugarloaf Key, Florida. Dr. Golbeck is a Professor at the University of Maryland in College Park and is Director of the Social Intelligence Lab. She is an expert in social networks, social media, privacy, and security on the web. As described in her Wikipedia entry, Dr. Golbeck "is known for her work on computational social network analysis. She developed methods for inferring information about relationships and people in social networks. Her models for computing trust between people in social networks are among the first in the field . . . [Dr.] Golbeck has received attention for her work on computing personality traits and political preferences of individuals based on their social network profiles. Her presentation at TEDxMidatlantic, discussing the need for new methods of educating users about how to protect their personal data, was selected as one of TED's 2014 Year in Ideas talks."[7] Dr. Golbeck's TED talk, "The curly fry conundrum: Why social media 'likes' say more than you might think," has received over 300,000 views on YouTube.[8]

12. Dr. Golbeck, like most members of modern society, must use the Internet to conduct routine affairs of daily life. Despite taking precautions to keep her personal information from being collected by third parties, Dr. Golbeck discovered Oracle tracking devices on multiple

[7] Wikipedia, *Jen Golbeck*, https://en.wikipedia.org/wiki/Jen_Golbeck [https://perma.cc/7Y2P-SU4C].

[8] TED, *Jennifer Golbeck: The Curly Fry Conundrum: Why Social Media "Likes" Say More Than You might Think*, YouTube (Apr. 3, 2014), https://www.youtube.com/watch?v=hgWie9dnssU [https://perma.cc/89JD-556N].

of her computers that she regularly uses for internet browsing and other activities. Additionally, on March 10, 2022, Dr. Golbeck received from Oracle an OARRR indicating Oracle had tracked, compiled, and analyzed her web browsing, geolocation, brick-and-mortar purchase and other activity and thereby created an electronic profile on her, attached hereto as Exhibit B. On information and belief, Oracle continues to track Dr. Golbeck's internet and offline activity, enrich the profile of her as described below, and make her personal information available to third parties without her consent. On information and belief, Dr. Golbeck visited websites where her electronic communications were intercepted by the use of Oracle JavaScript code, as described below.

13. The full scope and extent of Oracle's tracking and compiling of Dr. Golbeck's internet and offline activity and personal data resides with Oracle itself, is not fully disclosed by Oracle, and therefore must be determined through discovery from Oracle. Based on information known at this time, Dr. Golbeck alleges as follows.

14. Dr. Golbeck has searched for and viewed articles related to sensitive health issues on numerous health-specific websites. On information and belief, the bk-coretag javascript code was present on those websites at the time Dr. Golbeck read those articles, and that code transmitted to Oracle the URLs for the specific articles and web pages she accessed, as well as content she entered in search forms and other fields, add-to-cart actions, and other communications with websites along with a unique identifier that Oracle then used to associate that browsing history with a profile of her maintained by Oracle, which profile Oracle then provided unknown third parties access to. On information and belief, Dr. Golbeck's interest in the subject matter of those articles was made available and sold to those third parties. On information and belief, Oracle engaged in this conduct throughout the class period. Dr. Golbeck. The websites visited by Dr. Golbeck. where Oracle JavaScript tracking mechanisms have been detected include at least:

a. Healthline.com.

b. Psychiatry.org

15. Oracle has tracked Dr. Golbeck's activity on at least hundreds of other websites. Oracle tracking mechanisms, including "cookies," "pixels," and/or javascript code, as described

below at paragraphs 41-59, were present on those websites, including, on information and belief, at the time Dr. Golbeck accessed them. Those tracking mechanisms transmitted to Oracle the URL data coupled with unique identifiers that Oracle used to associate that browsing history with other data compiled into a data profile about her. On information and belief, the bk-coretag javascript code was present on a subset of websites at the time Dr. Golbeck read those articles, and that code transmitted to Oracle the URLs for the specific articles and web pages she accessed, as well as content she entered in search forms and other fields, add-to-cart actions, and other communications with websites. Oracle maintains a data profile concerning Dr. Golbeck, which Oracle provides direct or indirect access (e.g., via products or services derived from the profile) to unknown third parties. Oracle tracked Dr. Golbeck's activity on these websites, analyzed her browsing behavior and interests, and made that data, or information derived from that data (such as "segments" described at paragraphs 57, 64, and 74-76 below), via products or services derived from that profile, available to unknown third parties. On information and belief, Oracle engaged in this conduct throughout the class period. These websites visited by Dr. Golbeck include, but are not limited to:

a. Drugs.com

b. Health.com

c. Healthgrades.com

d. Mayoclinic.org

e. Verywellhealth.com

f. Verywellmind.com

g. Webmd.com

16. Oracle partnered with PlaceIQ to obtain, compile, and analyze hundreds of physical locations Dr. Golbeck had traveled to, as described above. Oracle likewise provided unknown third parties with "convenient access" to Dr. Golbeck's "real world movement data."[9] Dr.

[9] *PlaceIQ Data Now Available Through Oracle Data Cloud's BlueKai Marketplace*, PlaceIQ (July 13, 2016), https://www.placeiq.com/2016/07/placeiq-data-now-available-through-oracle-data-clouds-bluekai-marketplace/ [https://perma.cc/22T8-MVGZ].

Golbeck was neither aware of nor consented to this conduct. Through PlaceIQ, Oracle tracked Dr. Golbeck's activity at hundreds of specific locations, including:

a. retail locations;

b. restaurants;

c. gas stations;

d. banks—including the specific type of bank and branch, thereby revealing which banks Dr. Golbeck does business with.

17. Oracle obtained, compiled, and analyzed information about hundreds of Dr. Golbeck's credit card purchases, and then made that data, or information derived from that data, available to third parties through its Data Marketeplace. On information and belief, Oracle obtained, and continues to maintain in its systems, information about a vast swath of her credit card purchases, including reflecting purchases for travel to specific geographic locations, specific spending habits and preferences, and the "level" of spending she engages in. Dr. Golbeck was neither aware of nor consented to this conduct.

18. Oracle obtained, compiled, and analyzed information about Dr. Golbeck's charitable donations. This information was apparently granular enough to categorize Dr. Golbeck as a "religious donor."

19. Oracle associated the above information with a profile through its ID Graph, as described below, that contained detailed demographic information about her, as well as her name, email address, physical address, and phone numbers. As such, a person in possession of any of these identifiers, along with access to Oracle's dossier on her, could learn highly detailed, sensitive information about her. On information and belief, unknown third parties have actually accessed Dr. Golbeck's sensitive information in this manner.

20. Plaintiffs are informed and believed the OARRR reflects only a small portion of the information collected by Oracle on Plaintiffs since at least 2016. The OARRR does not list all of the specific pieces of Plaintiffs' personal information Oracle collected, despite the provisions of California Consumer Privacy Act section § 1798.110 (requiring Oracle to disclose to consumers the "specific pieces of personal information it has collected about that consumer."). The OARRR

fails to inform plaintiffs, for example, of the specific websites Oracle tracked Plaintiffs on, which can thus only be learned through discovery from Oracle.

21. **Defendant Oracle America, Inc.** ("Oracle" or "Defendant") is a United States public corporation incorporated under the laws of the State of Delaware and is registered with the State of California pursuant to California Civil Code § 1798.99.80 as a "data broker" residing at 500 Oracle Pkwy, Redwood City, California. On information and belief, Redwood City, California is, or has been for a majority of the class period, the principle place of business for Oracle and until at least December 2020, was the sole location it listed as its residence.

III. JURISDICTION AND VENUE

22. This Court has original jurisdiction over this matter pursuant to 28 U.S.C. § 1331 as it arises under the laws of the United States. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1332 and 1367 because this is a class action in which the matter or controversy exceeds the sum of $5,000,000, exclusive of interest and costs, and in which some members of the proposed Classes are citizens of a state different from Defendant.

23. This Court has personal jurisdiction over Defendant because Defendant conducts substantial business within this District and throughout the State of California, and was headquartered in Redwood City, California, for at least a substantial portion of the class period.

24. Venue properly lies with this Court pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2), because Plaintiff Katz-Lacabe resides within this District and because Oracle maintains substantial business operations in this District, and because a substantial part of the events or omissions giving rise to the claims described herein occurred in this District.

IV. CHOICE OF LAW

25. California law governs the substantive legal issues in this case for the California Subclass. The State of California has a significant interest in regulating the conduct of businesses operating within its borders. California, which seeks to protect the rights and interests of California and all residents and citizens of the United States against a company doing substantial business in California, has a greater interest in the claims of Plaintiffs and Class members than any

other state or country and is most intimately concerned with the claims and outcome of this litigation.

26. Until at least December 2020, Oracle's principal place of business is, or has been for the majority of the class period, Redwood City, California, where it is registered a data broker under California law, where it is functioning, during the majority of the relevant time period, as the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its marketing, software development, and major policy, financial, and legal decisions.

27. Oracle's privacy-invasive conduct as described herein emanated from, and was conceived and executed in, California.

28. Upon information and belief, the processes used to intercept, analyze, compile, store and sell Plaintiffs' data are or were performed in California. At least until December 2020, Oracle publicly represented that "Oracle Corporation and Oracle America, Inc., with their registered address at 500 Oracle Parkway, Redwood Shores, CA, 94065, United States, are responsible for the processing of your personal data."[10] The compiling of profiles on Plaintiffs takes or took place in California and the provision of those profiles to third parties takes or took place in California. With respect to Plaintiffs' intrusion upon seclusion and unjust enrichment claims, the last acts to make Oracle liable, including the creation, maintenance, and provision to third parties of these profiles, took place in California. Additionally, numerous Oracle employees who were involved in effectuating and/or directing the conduct described in this Complaint reside or are based in California.

29. That California has a greater interest in the claims of Plaintiffs and Class members than any other state or country and is most intimately concerned with the claims and outcome of this litigation is demonstrated by the scope of the California Consumer Privacy Act (CCPA). The legislators of California recognized California's great interest in—and responsibility for—the

[10] ,*Privacy @ Oracle Oracle Data Cloud Privacy Policy*, Oracle (Last Updated Oct. 20, 2020), https://web.archive.org/web/20201223013611/https:/www.oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html#responsible [https://perma.cc/WDX7-LNL6] (under "3. Who is responsible for your personal data")

conduct of technology companies operating within its borders, and in particular California's need to curtail the privacy-invasive practices of data brokers like Oracle residing or operating within California. The CCPA explicitly applies to the collection or sale personal information, and only exempts such conduct from its reach "if every aspect of that commercial conduct takes place wholly outside of California." *See* Cal. Civ. Code § 1798.145 (Exemptions). Moreover, pursuant to the CCPA, "commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, *no part of the sale of the consumer's personal information occurred in California*, and no personal information collected while the consumer was in California is sold." *Id.* (emphasis added). California legislators thus recognize that California has a great interest in regulating the sale of its consumers' information within California, even if that personal information was collected outside of California. Moreover, the Ninth Circuit has recognized that under California law, if the "conduct that 'creates liability' occurs in California, California law properly governs that conduct." *Oman v. Delta Air Lines, Inc.*, 889 F.3d 1075, 1079 (9th Cir. 2018).

30. On information and belief, the sale of Class members' personal information, through the Data Marketplace and the other Oracle products and services described herein, takes or took place in California, regardless of which state the Class member resides in. Accordingly, California has a great interest in Class members' claims against Oracle. To the extent there is any factual dispute about the location of the collection, compilation, analysis, or sale of Class members' personal data, that dispute must be resolved in discovery. Such discovery may encompass: the location of the "nerve center" of Oracles relevant business activities, the location where its high-level officers direct, control, and coordinate the corporation's relevant activities, the location of the development and implementation of the software and source code that effectuates Oracle's conduct described herein, and the location of the servers, electronic infrastructure, and other implements that are involved in effectuating Oracle's conduct described herein, including the collection, analysis, and sale of Class members' personal data.

31. Application of California law with respect to Plaintiffs' and Class members'

claims is reasonable and fundamentally fair because California has a state interest in the claims of the Plaintiffs and the Classes based upon Oracle's significant and ongoing contacts with California.

32. Under California's choice of law principles, which are applicable to this action, the common law of California applies to the common law claims of the California Subclass. Additionally, given California's significant interest in regulating the conduct of businesses operating within its borders, California's consumer protection laws may be applied to non-resident Plaintiffs and Class members.

33. In the alternative, he common law and statutory law of Florida applies to the Florida and FSCA classes.

V. INTRADISTRICT ASSIGNMENT

34. Pursuant to Civil L.R. 3-2(c), assignment to this division is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in this district. Defendant's conduct as described below is directed at Internet users and people throughout the United States, including in Alameda County, California.

VI. STATEMENT OF FACTS

35. Oracle is one of the world's largest data brokers, in addition to its prominent public facing business of database related software and data storage services, including "Oracle Cloud" that developers may use to build and run internet sites and mobile applications.[11] Oracle reaps great financial benefit from its conduct described herein; while the revenue attributable to its data broker businesses is not publicly disclosed, Oracle's market capitalization exceeds $227 billion.

36. As a data broker, Oracle facilitates the buying and selling of digital data, including personal information, among private commercial and governmental entities. Oracle operates a data management platform called the BlueKai Data Management Platform (now also known as "Oracle Data Management Platform" or "Oracle DMP"[12]), which includes two key features: the

[11] *Oracle Products, Solutions, and Services*, Oracle, https://www.oracle.com/products/ [https://perma.cc/96FG-AYQC].

[12] *See Integrating Oracle Eloqua and Oracle DMP*, Oracle (May 5, 2023),

Oracle Data Marketplace and the Oracle ID Graph. The Oracle Data Marketplace is one of the world's largest, if not the largest, commercial data exchange, with a broad impact upon the lives of most Americans and many millions of people worldwide.[13]

37. The Oracle ID Graph is a service product designed to provide "identity resolution," the process of "matching individual customer identities . . . and combining them into a single consistent and accurate customer profile."[14] Oracle's ID Graph "synchronizes" the vast amounts of personal data Oracle has amassed; that is, it matches personal data that can be determined to share a common origin with other personal data. This synchronizing allows Oracle to identify individuals and aggregate their many identifiers, which in turn facilitates further synchronizing of personal data with a high degree of confidence. As Oracle, in velveteen marketing language, describes it:

> The Oracle ID Graph helps marketers connect identities across disparate marketing channels and devices to one customer. Powered by the Oracle Marketing Cloud and Oracle Data Cloud, the Oracle ID Graph seamlessly pulls together the many IDs across marketing channels and devices that comprise a given person, enabling marketers to tie their interactions to an actionable customer profile. This ID enables the marketer to orchestrate a relevant, personalized experience for each individual across marketing channels and device types.[15]

38. Oracle and other data brokers act as central nodes in the "adtech" network, where massive volumes of personal information on the world's population is aggregated and used to identify and profile individuals for "targeted advertising" or other commercial and political purposes.

39. Oracle tracks the lives of the general public in a manner that is opaque, if not invisible, to the people it follows, as they have no direct relationship with Oracle. Oracle is registered as a "data broker" in California (and in other States), which is defined as "a business

https://docs.oracle.com/en/cloud/saas/marketing/eloqua user/pdf/OracleEloqua_BlueKai_AdminGuide.pdf [https://perma.cc/H5FA-BPQW] ("Important: Oracle BlueKai is now known as Oracle DMP").

[13] Giridhari Venkatadri, Piotr Sapiezynski, et al., *Auditing Offline Data Brokers via Facebook's Advertising Platform*, The World Wide Web Conference (May 13-17, 2019), https://lig-membres.imag.fr/gogao/papers/databrokers-measurement_finalCameraReady.pdf [https://perma.cc/H7XW-PWE2].

[14] *What Is a Customer Data Platform*, Oracle, https://www.oracle.com/bh/cx/customer-data-platform/what-is-cdp/ [https://perma.cc/FBW7-X8DP].

[15] *ID Management*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/id_management.html [https://perma.cc/LCW9-9PCH].

that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80. As such, Oracle does not even maintain a pretense of having directly obtained the consent of the subjects of its surveillance—i.e., the proposed Classes herein—who have no legal or practical ability to consent to Oracle's conduct.

40. Oracle's business model has long roots in the surveillance of ordinary citizens. Oracle takes its name from a CIA project codename. In 1977, Oracle's founder, Larry Ellison, was hired by the CIA to build a database; the CIA was Oracle's first customer. As of 2020, Oracle had contracts with all five branches of the military, and recent or pending contracts with the CIA, as well as substantial relationships with local law enforcement across the country. Surveillance is central to Oracle's history and development, and to its current business and marketing plan.

A. Oracle Employs Multiple Methods for the Collection of Personal Data from Unwitting Internet Users.

41. Operation of Oracle's ID Graph depends upon the accumulation of vast amounts of personal data concerning as many people as possible. Oracle utilizes multiple means to collect and aggregate the personal data of people worldwide, including the primary methods alleged in this subsection.

42. Oracle collects many types of personal information from Internet users including concrete identifiers such as names, home and work addresses, e-mail addresses, and telephone numbers. Oracle also amasses data about peoples' behavior, including the sites they visit online, their digital and offline purchases, where they shop, and how they pay for their purchases. Oracle gathers this personal information from a suite of its own Internet technologies, including cookies, tracking pixels, device identification, cross-device tracking, as well as from its acquisition of data from other parties. Oracle then processes, analyzes, and monetizes this data, as described below.

43. Cookies. Oracle deploys its own proprietary "cookies" which are pieces of software code sent by Oracle that are stored on Internet users' web browsers and collect information regarding Internet use. Oracle's cookies are frequently labeled "BlueKai," named after a start-up Oracle acquired in February 2014. Oracle's BlueKai cookies track online and

mobile app activity, obtaining data in real time and transmitting it back to Oracle's servers. When an Internet user visits a webpage or uses a mobile application, Oracle employs its BlueKai cookies to gather and transmit to itself information including the unique user ID, IP address, session time, number of sessions or visits, the URL or websites an Internet user has visited (*e.g.*, Referrer and Origin headers), hyperlinks clicked, and documents downloaded.[16] Oracle is able, with the use of algorithmic data processing, to use the data it gathers from BlueKai cookies (and, as explained below, which may also be associated with additional data from other sources) to infer a wide range of behavioral traits and information that it attributes to individual Internet users through persistent identifiers or other personal information of the Internet users—including their consumer preferences, income levels, and their politics.

44. <u>JavaScript</u>. Oracle utilizes a proprietary software device, referred to as "bk-coretag.js" JavaScript code, to "extract," or intercept, "user attributes," which include the contents of users' communications with websites, and secretly sends them to Oracle while the users are in the process of communicating with those websites. Oracle's technical documentation explains that bk-coretag.js JavaScript code deployed by Oracle collects "user attributes" "such as product views, purchase intent, [and] add-to-cart actions"[17] and other communications that users have with websites and simultaneously copies and sends those communications to Oracle.

45. Oracle places the bk-coretag.js JavaScript code on Internet users' electronic devices when they browse a website that contains certain Oracle code. When an individual Internet user visits a webpage, his or her browser sends a message called a "GET request" to the webpage's server. The GET request tells the website what information is being requested and also instructs the website's server to send the information back to the user. The bk-coretag.js JavaScript code then communicates with Oracle's servers and source code by sending separate "GET" requests to

[16] Martin Degeling & Jan Nierhoff, *Tracking and Tricking a Profiler Automated Measuring and Influencing of Bluekai's Interest Profiling*, Workshop on Privacy in the Electronic Society (Oct. 15, 2018), https://dl.acm.org/doi/pdf/10.1145/3267323.3268955 [https://perma.cc/7UVK-ALU9].

[17] *Oracle Data Cloud Core Tag Implementation*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/DataIngest/coretag_implementation.html [https://perma.cc/8XVU-8Z2F].

Oracle that contain copies of contents in the initial “GET” request being sent by the user’s browser to the website they are visiting.

46. Oracle uses the bk-coretag.js JavaScript code to intercept the contents of Internet users’ communications with websites as follows:

a. When a user opens an Internet webpage that contains certain code, a request is sent by the user’s browser to Oracle’s servers to fetch the bk-coretag.js JavaScript file.

b. The bkcoretag.js code then triggers a series of additional network “GET” requests.

c. As part of these “GET” requests, the bk-coretag.js code intercepts the contents of the user’s communications with the browser and simultaneously copies those contents and sends them to Oracle.

47. Through this practice, Oracle is able to intercept substantive communications between internet users and websites, including, inter alia: [18]

a. the URLs being browsed by the Internet user as well as the referrer URL;

b. webpage title;

c. webpage keywords;

d. the exact date and time of the website visit;

e. the IP address of the user’s computer;

f. product page visits;

g. “purchase intent”[19] signals;

h. “add-to-cart actions”; and

i. data entered by the user into forms on the website.

[18] *Data Ingest*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/data_ingest.html [https://perma.cc/99JS-5Z64].

[19] Oracle’s technical documentation does not appear to define the term “purchase intent,” however an Oracle document describes “Interest and intent signals” as including “search, page views, and price comparison.” *See Activation Playbook*, Oracle (2020), https://www.oracle.com/za/a/ocom/docs/cx-activation-vertical-playbook-2020.pdf [https://perma.cc/TYS5-NKX4].

48. The bk-coretag.js code also sends to Oracle the Internet user's login status and "hashes" of the user's email address and phone number.[20] Oracle attributes the communications to specific individuals using identifiers, such as email address, phone number, or account ID, and then uses this data to enrich its user profiles and ID Graph and classify users into categories for targeting.[21]

49. Oracle's technical documentation also explains that bk-coretag.js engages in "synchronous" communication interception, i.e., interception while the communication is in transit, which "[s]ends data to the Oracle Data Cloud platform as quickly as possible . . . while the web browser loads."

50. Oracle's bk-coretag.js JavaScript code has been recognized by security researchers as a tracking mechanism for surreptitiously monitoring and intercepting user's internet communications and activity. It has been described as "click interception script" that intercepts clicks by users on webpages,[22] and as an online activity "tracker" that can "learn a sizable chunk of the browsing history of a given user, and likely without their knowledge."[23]

51. Tracking Pixels. Another tool utilized in Oracle's digital tracking efforts are "tracking pixels." Tracking pixels are pieces of code that are embedded into webpages and mobile applications built with Oracle's technology, such as Oracle Cloud. Oracle tracking pixels are essentially invisible to Internet users because they are hidden within the code of a webpage and activate (or "fire") whenever the page is opened, regardless of and prior to any pretense of consent

[20] According to Oracle, "Hashing is a form of encryption used for swapping data between integrated data management systems." *See Hashing Identifier*, Oracle, https://docs.oracle.com/en/cloud/saas/marketing/eloqua-user/Help/General/HashingIdentifier.htm [https://perma.cc/C59Q-X4PC].

[21] *Oracle Data Cloud Core Tag Implementation*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/DataIngest/coretag_implementation.html [https://perma.cc/8XVU-8Z2F].

[22] Mingxue Zhang, Wei Meng, et al., *All Your Clicks Belong to Me: Investigating Click Interception on the Web*, Proceedings of the 28th USENIX Security Symposium (Aug. 14-16, 2019), https://www.usenix.org/system/files/sec19fall_zhang_prepub.pdf [https://perma.cc/8A9V-URWL].

[23] *See* Zhonhao Yu, Sam Macbeth, et al., *Tracking the Trackers*, World Wide Web Conference (April 11-15, 2016), http://josepmpujol.net/public/papers/pujolTrackingTheTrackers.pdf [https://perma.cc/WT3W-TW5U].

being sought. Unlike cookies, tracking pixels cannot be disabled. When a user visits a site with an Oracle pixel, the company receives, at minimum, the full URL, time zone, screen resolution, browser window resolution, and title of the webpage.[24] Consequently, if a person visits, for example, a specific product page on a retailer's website, Oracle instantly knows about it and, as with cookies, adds the information to the person's profile in Oracle's database. Nor are pixels confined to websites: Oracle pixels are in marketing emails from numerous companies—when the email is opened, the pixels identify the specific reader and the underlying marketing campaign.[25]

52. This data collection is not dependent upon any relationship that an Internet user may or may not have with Oracle. In fact, Oracle primarily collects data through its BlueKai cookies and pixels from persons having no privity whatsoever with Oracle. Even privacy-conscious users who endeavor to understand the origins of Oracle cookies may not know Oracle is amassing data about them because Oracle's cookies and pixels do not bear the company's name.

53. Oracle's cookies and tracking pixels are pervasive throughout the Internet. [26] Oracle has agreements with numerous high-traffic websites like the New York Times, ESPN, and Amazon to place cookies and/or pixels on their websites.[27] By blanketing popular websites with these tracking tools, Oracle reaches a substantial percentage of Internet users—Oracle cookies are found on over 20 percent of the top 10,000 websites[28] and more than 48 thousand websites.[29]

[24] *Device Fingerprints and Custom Sign In Pages*, Oracle, https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/use-device-fingerprints.html#GUID-17B61B5F-7937-4830-8368-075EE2001BDF [https://perma.cc/56VS-XQFU].

[25] *Activating Eloqua Email Marketing Data*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/ManagingTaxonomy/ingest_partners/eloqua_email_data_activation.html [https://perma.cc/A8ZZ-HLF7].

[26] *Host Search Results: bluekai.com*, Cookiepedia, https://cookiepedia.co.uk/host/bluekai.com [https://perma.cc/RHA9-KTRB].

[27] Wolfie Christl (@wolfiechristl), Twitter (Mar. 23, 2018, 12:55 PM), https://twitter.com/WolfieChristl/status/977272603038633985?s=20.

[28] Additionally, a Dutch action against Oracle alleges its cookies are found on at least 28 of 100 of the most popular websites in the Netherlands. *Writ (For The Main Action)*, The Privacy Collective (Aug. 26, 2020), https://theprivacycollective.nl/wp-content/uploads/2020/11/Writ-of-Summons-English-translation-26-August-2020.pdf [https://perma.cc/4AKV-XNRY] (¶ 427).

[29] *Oracle BlueKai*, NerdyData, https://www.nerdydata.com/reports/oracle-bluekai/e99ff880-6d16-45d1-94c7-6cce7ae1571d [https://perma.cc/64ME-U27H].

54. Device Identification. Oracle tracks users by harvesting and exfiltrating user "device identifiers." Oracle is able to track Class members' online activities by collecting identifiers tied to their devices. These identifiers include IMEI (International Mobile Equipment Identity), MAC address (Media Access Control address), and Mobile Advertising ID (MAID) such as Advertising Identifier (IDFA) on iOS and Advertising ID (ADID) on Android devices.[30]

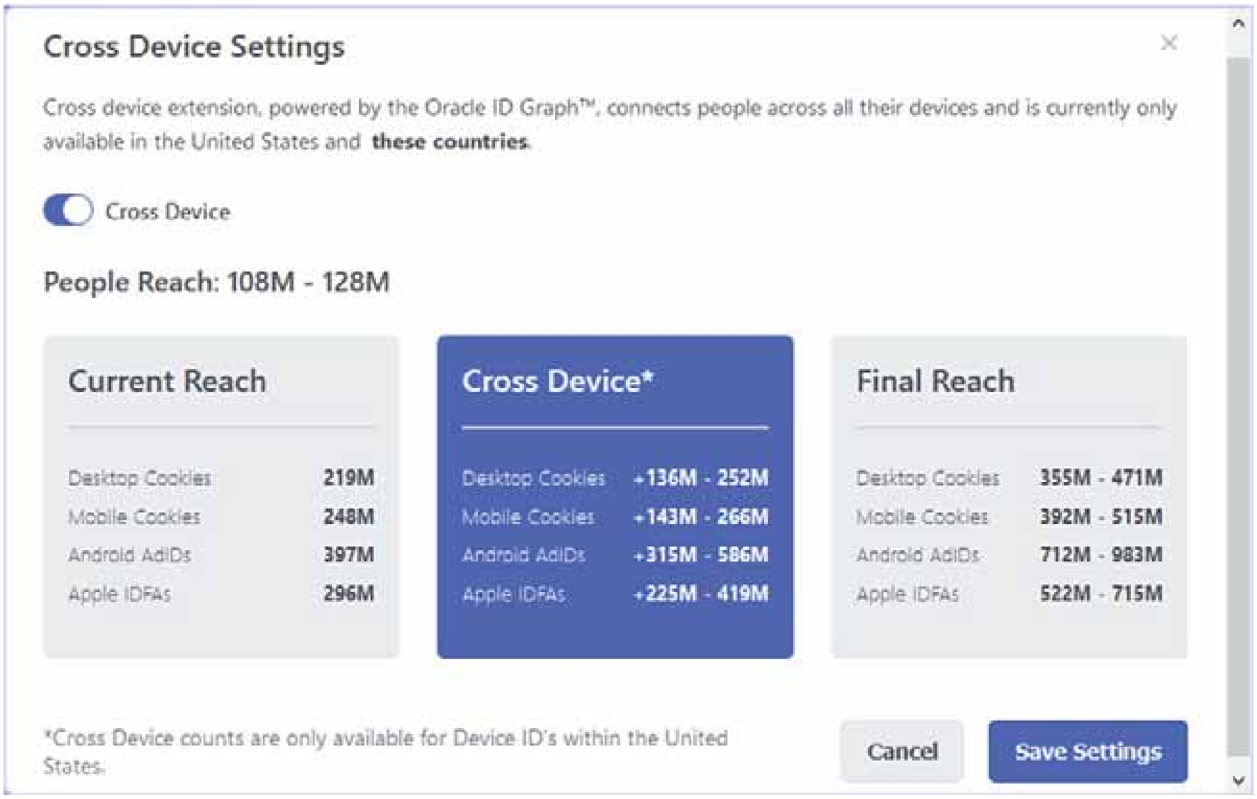
55. Cross-device Tracking. Oracle monitors Class members' activities across their devices through cross-device tracking. When Class members shop online at home on their iPad, read the news on their iPhone during their commute, and visit sites on their laptop at work, Oracle monitors and collects their movements.[31] Oracle also tracks activity through television and touts its ability to monitor viewing habits and measure the effectiveness of advertising in video games.[32] Oracle thereby allows its customers to target Plaintiffs and Class members *across their devices* with the flip of a switch, as this graphic from Oracle illustrates:[33]

[30] *Fingerprinting Types*, Oracle, https://docs.oracle.com/cd/E52734_01/oaam/AAMAD/finger.htm#AAMAD9008 [https://perma.cc/252P-6BN9].

[31] *ID Management*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/id_management.html [https://perma.cc/LCW9-9PCH].

[32] Glenn Bean, *How Moat Reach Captures Cross-Platform Reach and Frequency-and Why it's Better Than What You Have Today*, Oracle Advertising Blog (Jun. 3, 2020), https://blogs.oracle.com/advertising/post/how-moat-reach-captures-cross-platform-reach-and-frequencyand-why-its-better-than-what-you-have-today [https://perma.cc/YMG6-DT8N]; *TV & Digital Campaign Measurement*, Oracle, https://www.oracle.com/cx/advertising/measure-campaign-effectiveness/cross-platform-measurement/ [https://perma.cc/W55S-ZUC9] ; *Industry first: In-game measurement for 3D advertisements*, Oracle, *https*://www.oracle.com/cx/advertising/data-enrichment-measurement/#ingame-measurement [https://perma.cc/9DEK-9FJV].

[33] *Creating Audiences*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/Audiences/create_audience.html [https://perma.cc/K6F2-NPZF].



Cross Device Settings

Cross device extension, powered by the Oracle ID Graph™, connects people across all their devices and is currently only available in the United States and **these countries**.

Cross Device

People Reach: 108M - 128M

	Current Reach	Cross Device*	Final Reach
Desktop Cookies	219M	+136M - 252M	355M - 471M
Mobile Cookies	248M	+143M - 266M	392M - 515M
Android AdIDs	397M	+315M - 586M	712M - 983M
Apple IDFAs	296M	+225M - 419M	522M - 715M

*Cross Device counts are only available for Device ID's within the United States.

56. AddThis. AddThis is a widget, or a piece of code that web developers incorporate into a website that provides a graphical user interface that displays information and provides a means for a user to interact with the website, which Oracle acquired in 2016. With an AddThis enabled website, Internet users can bookmark or post the webpage to their various social media platforms including Facebook, Pinterest, and Twitter. These plugins, which are free, are ubiquitous: AddThis is currently used on 15 million websites and purports to offer “insight into the interests and behaviors of over 1.9 billion web visitors,” and its “vast global footprint reaches 96% of the U.S. web.”[34] Whenever an Internet user visits a website with an AddThis plugin, the user is subjected to cookies and pixels, without any notice or practical ability for detection, and as a result, Internet users are unaware that Oracle is tracking and recording their online activity for purposes of identifying the Internet users and their activities to Oracle and its customers. Recent forensic analysis has confirmed that AddThis is ubiquitous and tracks data from sites related to sensitive health and personal safety information: AddThis trackers were found on more than 4,000

[34] *About Us*, AddThis (2022), https://www.addthis.com/about/ [https://perma.cc/JK9N-3W3Z].

popular websites, as well as four states' coronavirus information pages.[35] AddThis trackers were also found on websites with resources for undocumented immigrants, domestic violence survivors, and the LGBTQ community.[36] Human Rights Watch, concerned about Oracle's collection of data from children, has noted that:

> . . . AddThis does much more than encourage social media traffic. Whether or not a person clicks on the "share" button, AddThis instantly loads dozens of cookies and tracking pixels on website visitors' browsers, like nesting dolls, each collecting and sending user data to Oracle and to dozens of other AdTech companies to profile and target a person or a child with behavioral advertising that follows them across the internet.[37]

57. Datalogix. In 2014, Oracle acquired Datalogix, an information broker specializing in profiling people based on their purchases at brick-and-mortar retailers, primarily by purchasing and aggregating data from retailers' loyalty programs. In 2019, an Oracle executive explained the colossal scale of this data as including, "115 million U.S. households, 10 billion SKU-level transactions, over 1,500 leading brands, and $5 trillion in consumer spending data."[38] Datalogix's coverage was found by academic researchers to be up to 76.2% in the U.S. and 43.6% in the U.K.[39] Datalogix data is now referred to as "Oracle Datalogix (DLX) data" and is described by Oracle as "the premier solution when looking for offline purchase- and activity-based audiences."[40] Among Oracle's current product offerings is the "Datalogix Profile Analysis" which

[35] Aaron Sankin & Surya Mattu, *The High Privacy Cost of a "Free" Website*, The Markup (Sept. 22, 2020, 6:00 AM ET), https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites [https://perma.cc/X66F-79D6].

[36] *Id.*

[37] *"How Dare They Peep into My Private Life?" Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*, Human Rights Watch (May 25, 2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments [https://perma.cc/3R2D-46PM].

[38] *Audience Targeting with Oracle: Q&A with Oracle Data Cloud's Dan Loewenberg*, Spot X (Mar. 21, 2019), https://www.spotx.tv/resources/blog/product-pulse/audience-targeting-with-oracle-qa-with-oracle-data-clouds-dan-loewenberg [https://perma.cc/6T3N-TY2Z].

[39] Giridhari Venkatadri, Piotr Sapiezynski, et al., *Auditing Offline Data Brokers via Facebook's Advertising Platform*, The World Wide Web Conference (May 13-17, 2019), https://lig-membres.imag.fr/gogao/papers/databrokers-measurement_finalCameraReady.pdf [https://perma.cc/H7XW-PWE2].

[40] *Datalogix by Oracle Data Cloud*, Twitter, https://partners.twitter.com/en/partners/datalogix-by-oracle-data-cloud [https://perma.cc/N855-D5VV].

provides advertisers with “Demographic Segments,” “Lifestyle Segments, Retail Behavioral Segments, and Purchase Behavioral Segments” on Internet users.[41]

58. Data From Third Parties. Oracle enhances the personal information that it collects from Internet users with personal information collected and sold by other third-party data brokers. The personal information Oracle amasses through its tracking technologies together with the personal information collected by third parties includes billions of data points on more than 300 million users, or over 80% of the entire U.S. population.[42]

59. When an Internet user uses a website employing the Oracle tracking technologies described above, Oracle can track and store behavioral activity and personal information, including, but not limited to, home location, age, income, education, family status, hobbies, weight, and what the user bought at a brick-and-mortar business yesterday afternoon. Internet users are not made aware of, and therefore cannot consent to, use of their information to facilitate Oracle’s personal identification enterprise, the “Oracle ID Graph.”

B. Oracle Uses The Personal Data of Internet Users To Fuel Its Personal Identification and Profiling Product “Oracle ID Graph.”

60. Oracle has developed the “Oracle ID Graph” using the vast stores of personal data it has accumulated. Oracle designed the Oracle ID Graph to have the capability of identifying Internet users and compiling personal data associated with them, including so-called “anonymous” data which Oracle re-identifies to specific individuals. Oracle makes the Oracle ID Graph available for sale to private and governmental purchasers on its Data Marketplace.

61. In April 2015, Oracle unveiled Oracle ID Graph as a new feature of the BlueKai data management platform.[43] The introduction of Oracle ID Graph permitted the compiling of an

[41] *Using the Datalogix Profile Analysis Dashboard*, Oracle, https://docs.oracle.com/en/cloud/saas/marketing/cx-audience-user/AudienceInsight_DLXDashboard.htm#Using [https://perma.cc/G4DM-BWR8].

[42] *Oracle Data Marketplace*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/AudienceDataMarketplace/AudienceDataMarketplace.html [https://perma.cc/27S8-GX7H].

[43] *Oracle Energizes Its Marketing Cloud With New Features*, Forbes (Apr. 7, 2015), https://www.forbes.com/sites/greatspeculations/2015/04/07/oracle-energizes-its-marketing-cloud-with-new-features/?sh=1db7452b7852 [https://perma.cc/WT53-CYEH].

Internet user's various disaggregated identifiers. Previously, because browsers, devices, and mobile applications each use a different identifier, identification of users was typically limited to a single device. The Oracle ID Graph processes available personal data, digital identifiers (such as "browser cookies, mobile advertising IDs, IP addresses, and console IDs"), and concrete identifiers (such as "hashed first names, last names, postal addresses, email addresses, and telephone numbers") to identify and establish "a single, universal view of identity" for each user.[44] In addition to connecting and associating multiple browser and device identifiers, the Oracle ID Graph combines these identifiers with demographic, behavioral, and biographic data, ranging from marital status to hair type to college major to household location, to enhance the profiles of individuals within its ID Graph.[45]

62. Oracle has described its ID Graph as the "backbone technology [that] powers all Oracle Data Cloud solutions," allowing Oracle's customers to track individual people "seamlessly across devices (desktop and mobile) and channels (offline and online) via more than 200 media and marketing platforms, including the largest and fasted-growing consumer platforms."[46]

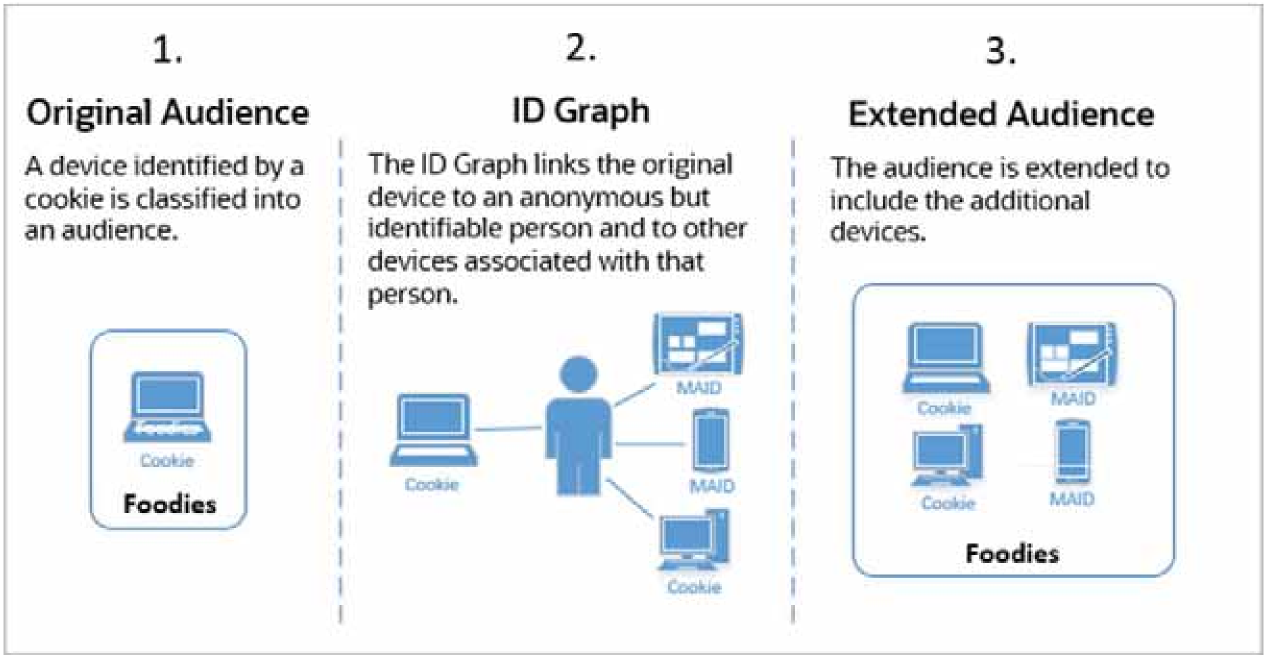
63. The Oracle ID Graph is an example of the practice known in the adtech industry as "identity resolution." As Oracle explains, the Oracle ID Graph lets its customers "connect identities across disparate marketing channels and devices to one customer" by "seamlessly pull[ing] together the many IDs across marketing channels and devices that comprise a given

[44] *12 Must-Ask Questions to Separate Fact From Fiction*, Oracle (2018), https://www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf [https://perma.cc/WW3A-HVBA].

[45] *Activation Playbook*, Oracle (2020), https://www.oracle.com/ca-fr/a/ocom/docs/cx-activation-vertical-playbook-2020.pdf [https://perma.cc/TYS5-NKX4].

[46] *Powered by Oracle ID Graph*, Oracle, https://web.archive.org/web/20180826201234/https://www.oracle.com/applications/customer-experience/data-cloud/solutions/id-graph.html [https://perma.cc/SG2R-VQKS]. Oracle further describes the ID Graph as follows: "The Oracle ID Graph is not a product but it is a foundational capability or technology that power[s] the Oracle [Bluekai Data Management Platform]. All linkages in Oracle ID Graph are continuously validated and scored, which changes dynamically based on a proprietary algorithm to the input . . . . Oracle ingests massive amounts of IDs across cookies, login, HH, email, and mobile ad IDs on a weekly or sometimes daily basis from ID data partners." *See Unite Disparate Data to Make It Actionable*, Oracle, https://web.archive.org/web/20210119032758/https://www.oracle.com/data-cloud/products/data-management-platform/id-graph.html [https://perma.cc/Y5A5-MXL3].

person, enabling marketers to tie their interactions to an actionable customer profile."[47] The following illustration from Oracle describes this process:[48]


1.
Original Audience
A device identified by a cookie is classified into an audience.
Cookie
Foodies
2.
ID Graph
The ID Graph links the original device to an anonymous but identifiable person and to other devices associated with that person.
Cookie
MAID
MAID
Cookie
3.
Extended Audience
The audience is extended to include the additional devices.
Cookie
MAID
Cookie
MAID
Foodies

64. Oracle's identity resolution process consists generally of three steps:

a. ***First,*** Oracle filters the data it collects, from BlueKai cookies, pixels and other sources, into millions of individual profiles on Class members. Data from, *inter alia*, "$90B in transactions tied to real people every week," "digital ID graphing on 115MM+ households," and "a global network of 15MM websites" is validated, compared, and combined into "a single, universal view of identity." The ensuing profiles are exceedingly detailed. They include digital identifiers like "browser cookies, mobile advertising IDs, IP addresses, and console IDs," and hard data such as "hashed first names, last names, postal addresses, email addresses, and telephone numbers."[49] This is in addition to the details that Oracle layers onto these core identifiers, including offline and geolocation data. As Oracle describes it, the "promise" of the ID

[47] *ID Management*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/id_management.html [https://perma.cc/LCW9-9PCH].

[48] *Creating Audiences*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/Audiences/create_audience.html [https://perma.cc/K6F2-NPZF] (the reference to "MAID" refers to a "mobile advertising ID").

[49] *12 Must-Ask Questions to Separate Fact From Fiction*, Oracle (2018), https://www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf [https://perma.cc/WW3A-HVBA].

Graph "is to connect identifiers to the consumer online and offline. Offline data ties the identity graph to *real people living at a real address*, not just a mixture of device IDs and cookies. Identity graphs built from offline *and* online signals are better connected and validated."[50]

b. ***Second,*** Oracle applies analytics to extract yet more information from the profiles it has created. An Oracle profile has hundreds or thousands of data points; Oracle then infers from this raw data that, for example, a person isn't sleeping well, or is experiencing headaches or sore throats, or is looking to lose weight, and thousands of other invasive and highly personalized inferences.[51]

c. This process provides Oracle with a virtual panopticon: Oracle purports to have vision on virtually everything ascertainable in electronic form about Class members, from where they live, to the media they consume, to the things they buy, to the views they hold.[52] The following examples illustrate the extraordinary breadth of the data that Oracle's customers can access via Oracle ID Graph:

> *Address:* Oracle has an address for over 110 million households, and lets clients target households within a radius of a given location.[53]
>
> *Life Events:* Oracle can target based on major life events, including marriage, childbirth, job changes, and graduation.[54]
>
> *Education:* Oracle segments by degree obtained, type of school (*e.g.* public, private, community college, online), and even major.[55]
>
> *Purchase History:* Oracle can filter for specific purchases—made both in brick-and-mortar establishments and online—such as "Alcohol Beverage purchase based modeled audiences," including micro-targeting categories tracking people's alcohol use habits, such as "Malt Beverage Buyers" or "Wine or Liquor Store Top Spenders."[56]

[50] *Id.*(emphasis added).

[51] *Oracle Data Cloud Health and Wellness Segments (US only)*, Oracle (Last Updated Oct. 14, 2020), https://www.oracle.com/a/ocom/docs/corporate/health-and-wellness-segments.pdf [https://perma.cc/37T2-FG4Q].

[52] *Activation Playbook*, Oracle (2020), https://www.oracle.com/za/a/ocom/docs/cx-activation-vertical-playbook-2020.pdf [https://perma.cc/TYS5-NKX4].

[53] *Id.*

[54] *Id.*

[55] *The Audience Playbook*, Oracle, at 11 (Aug. 2016), http://online.pubhtml5.com/mdhz/hgpp/#p=11 [https://perma.cc/L6WS-ND8L].

[56] *Alcohol and Beverage Digital Audiences and Contextual Segments*, Oracle, https://www.oracle.com/middleeast/a/ocom/docs/beverage-digital-audiences-contextual-segments.pdf [https://perma.cc/YEL7-DKG6].

> *Health & Wellness:* Oracle segments people based on intimate information, including a person's views on their weight, hair type, sleep habits, and type of insurance.[57] Other categories appear to be proxies for medical information that Oracle purports not to share, like "Emergency Medicine," "Imaging & Radiology," "Nuclear Medicine," "Respiratory Therapy," "Aging & Geriatrics" "Pain Relief," and "Allergy & Immunology."[58]

d. ***Third,*** Oracle matches the data provided by its customers to the existing profiles of individuals it has developed. Using "Oracle OnRamp," the company "ingests [customers'] PII [personally identifiable information] and matches it to 115MM U.S. households, first names, last names, and telephone numbers."[59] Oracle clients can then target (or exclude) Class members based on attributes in Oracle profiles, and purchase yet more customer information from the Oracle Data Marketplace.

e. The matching process also helps Oracle's clients to knit together aspects of their own data sources. For instance, tying previously siloed online and offline information to an Oracle profile might reveal the user who last week visited a business's website is the same person who yesterday made purchases at a particular brick-and-mortar store belonging to that same business.[60] The image below illustrates the process.[61]

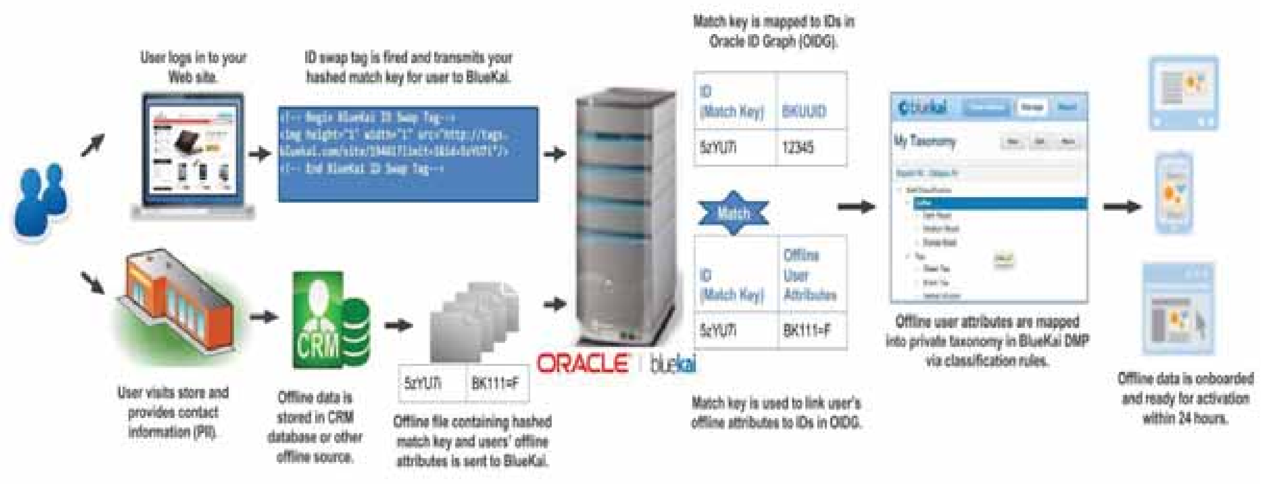
[57] *Oracle Data Cloud Health and Wellness segments (US only)*, Oracle, (Last updated Oct. 14, 2020) https://www.oracle.com/a/ocom/docs/corporate/health-and-wellness-segments.pdf [https://perma.cc/37T2-FG4Q].

[58] *Id.*

[59] *12 Must-Ask Questions to Separate Fact From Fiction*, Oracle (2018), https://www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf [https://perma.cc/WW3A-HVBA].

[60] *Id.*

[61] *Offline Match Integration*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/DataIngest/offline_match.html [https://perma.cc/2QXQ-TNY4]. Oracle offers clients other ways to ingest customer data, but regardless of means the result—uploading customer data to the Oracle Data Cloud—is the same. The other options are summarized at *Data Ingest*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/data_ingest.html [https://perma.cc/S2FZ-EYLD].


User logs in to your Web site.
ID swap tag is fired and transmits your hashed match key for user to BlueKai.
User visits store and provides contact information (PII).
Offline data is stored in CRM database or other offline source.
CRM
Offline file containing hashed match key and users' offline attributes is sent to BlueKai.
ORACLE
bluekai
Match key is mapped to IDs in Oracle ID Graph (OIDG).
Match
Match key is used to link user's offline attributes to IDs in OIDG.
bluekai
My Taxonomy
Offline user attributes are mapped into private taxonomy in BlueKai DMP via classification rules.
Offline data is onboarded and ready for activation within 24 hours.

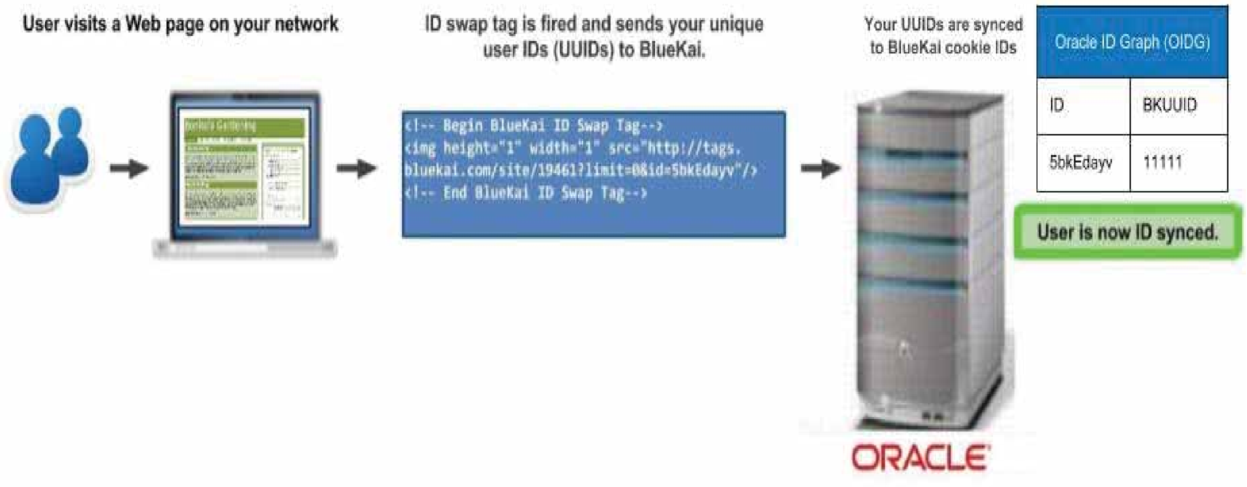
```
<!-- Begin BlueKai ID Swap Tag-->
<img height="1" width="1" src="http://tags.
bluekai.com/site/19461?limit=0&id=5zYUTi"/>
<!-- End BlueKai ID Swap Tag-->
```

5zYUTi	BK111=F

ID (Match Key)	BKUUID
5zYUTi	12345

ID (Match Key)	Offline User Attributes
5zYUTi	BK111=F

65. Oracle ID Graph relies on "ID swapping" to "synchronize" or match unique user IDs (UUIDs) of Class members between Oracle Data Cloud Platform and its clients. Oracle ID Graph employs a variety of deterministic and probabilistic matching techniques to this end.[62] The combination of deterministic and probabilistic techniques to construct the Oracle ID Graph is one of its distinguishing features.[63] This process includes the following technical features:


User visits a Web page on your network
ID swap tag is fired and sends your unique user IDs (UUIDs) to BlueKai.
Your UUIDs are synced to BlueKai cookie IDs
User is now ID synced.
ORACLE

```
<!-- Begin BlueKai ID Swap Tag-->
<img height="1" width="1" src="http://tags.
bluekai.com/site/19461?limit=0&id=5bkEdayv"/>
<!-- End BlueKai ID Swap Tag-->
```

Oracle ID Graph (OIDG)	
ID	BKUUID
5bkEdayv	11111

[62] *Deterministic and Probabilistic Data Matching*, Oracle (2010), https://docs.oracle.com/cd/E19182-01/821-0919/ref_sme-deter-probl_c/index.html [https://perma.cc/NCL3-QYHD].

[63] Audrey Rusch, *When it Comes to Identity, Probabilistic or Deterministic is Not the Question*, Oracle, (Aug. 19, 2019), https://blogs.oracle.com/advertising/post/when-it-comes-to-identity-probabilistic-or-deterministic-is-not-the-question [https://perma.cc/5EQE-REXV].

a. Oracle employs a "tag" to exfiltrate Class members' personally identifiable information such as email addresses, phone numbers, physical addresses, account numbers, Twitter handles, and other information to Oracle for a deterministic match.[64] Even if the personally identifiable information is hashed before being exfiltrated to Oracle, it can be easily reversed and thus does not provide any privacy as compared to no hashing.[65]

b. Oracle employs "cookie sync" technology[66] to link cookie-based identifiers of Class members between Oracle Data Cloud Platform and its clients for a deterministic match.[67] Cookie syncing is used by Oracle to circumvent the security feature of web browsers called "Same Origin Policy" that aims to prevent data sharing between different parties.[68] Cookie syncing also helps Oracle circumvent privacy features in web browsers, such as Safari, that block third-party cookies.[69]

c. For Class members using mobile apps where cookies may not be present, Oracle uses Mobile advertising IDs (MAIDs) that are derived from mobile apps (e.g., Identifier for Advertisers [IDFA] on iOS[70] and Google Advertising ID (AAID) on Android[71]) for a

[64] *ID Swapping*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/IDManagement/id_swap.html [https://perma.cc/54R4-JKAM].

[65] Gunes Acar, *Four Cents to Deanonymize: Companies Reverse Hashed Email Addresses*, Freedom to Tinker (Apr. 9, 2018) https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/ [https://perma.cc/4J9T-2Q6G].

[66] *Oracle BlueKai Glossary*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Glossary/OracleBlueKaiGlossary.htm [https://perma.cc/NBK7-N2H7].

[67] Zach Rodgers, *In A Year Of Data Disruption, Oracle Places Its Bets*, Ad Exchanger (Sept. 9, 2020) https://www.adexchanger.com/adexchanger-talks/in-a-year-of-data-disruption-oracle-places-its-bets/ [https://perma.cc/VV9E-TCXR].

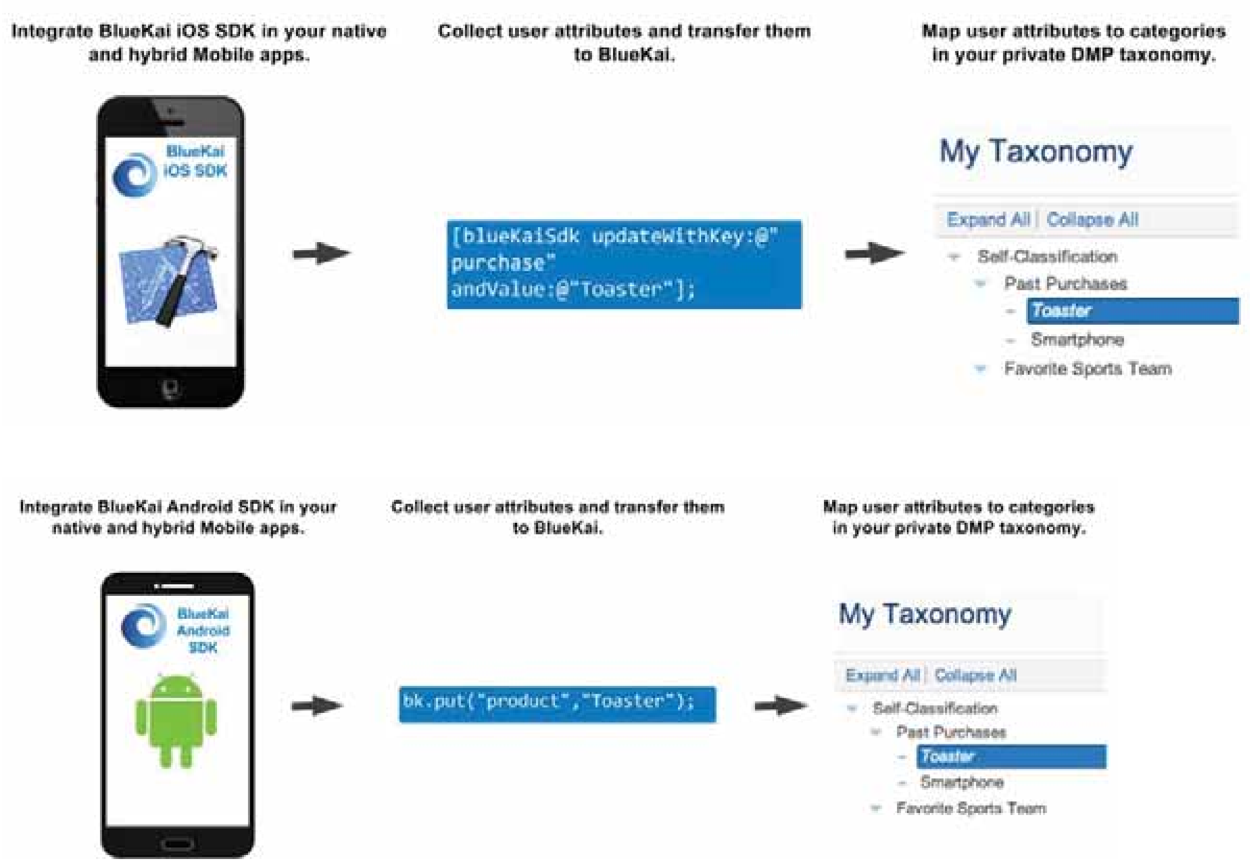
[68] Panagiotis Papadopoulos, Nicolas Kourtellis, et al., *Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask*, The World Wide Web Conference (May 13-17, 2019), https://arxiv.org/pdf/1805.10505.pdf [https://perma.cc/F4UJ-CHZ8].

[69] Quan Chen, Panagiotis Ilia, et al., *Cookie Swap Party: Abusing First-Party Cookies for Web Tracking*, The Web Conference (April 19-23, 2021), https://www3.cs.stonybrook.edu/~mikepo/papers/firstparty.www21.pdf [https://perma.cc/W3MH-GU8X].

[70] *iOS SDK*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/MobileIntegrations/ios_sdk.html [https://perma.cc/3475-3X3B].

[71] *Android SDK*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/MobileIntegrations/android_sdk.html [https://perma.cc/GB3K-ELJA].

deterministic match.[72] MAIDs are linked by data brokers to "a person's full name, physical address, and other personal identifiable information (PII)".[73]



Integrate BlueKai iOS SDK in your native and hybrid Mobile apps.

Collect user attributes and transfer them to BlueKai.

```
[blueKaiSdk updateWithKey:@"
purchase"
andValue:@"Toaster"];
```

Map user attributes to categories in your private DMP taxonomy.

Integrate BlueKai Android SDK in your native and hybrid Mobile apps.

Collect user attributes and transfer them to BlueKai.

```
bk.put("product","Toaster");
```

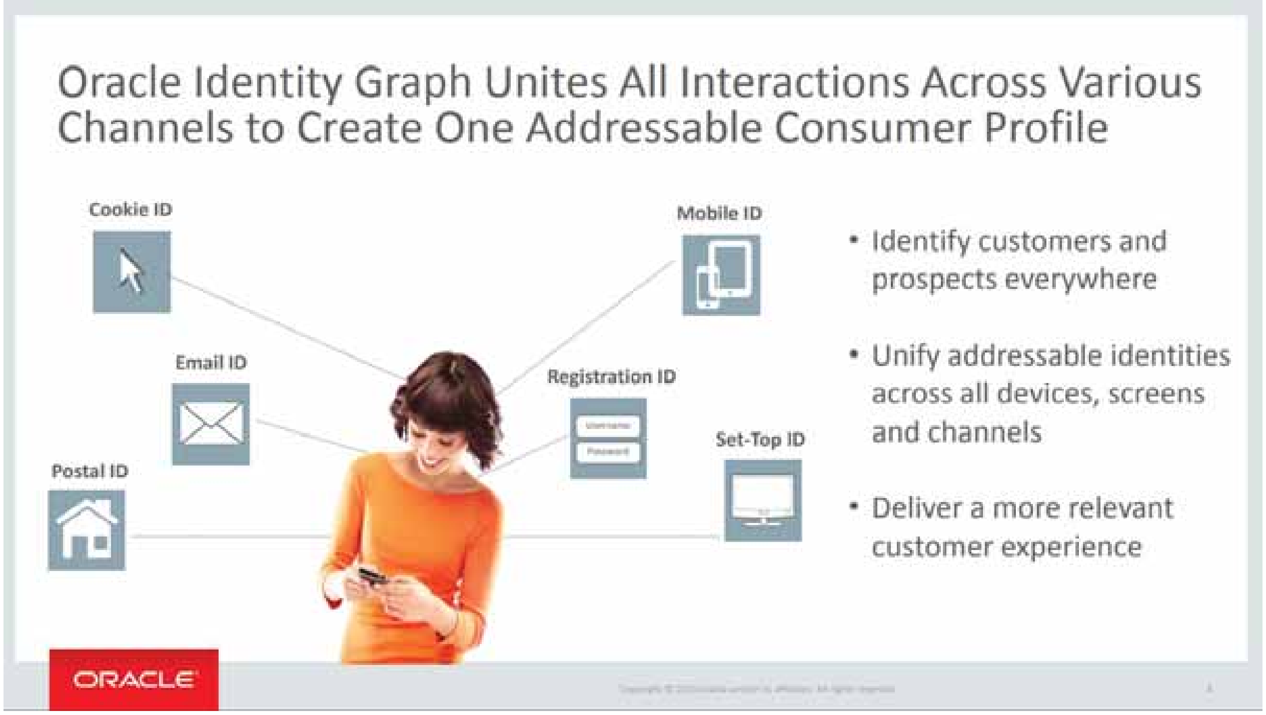
Map user attributes to categories in your private DMP taxonomy.

66. Oracle's marketing materials[74] make explicit that Oracle's ID Graph "Unites All Interactions Across Various Channels to Create One Addressable Consumer Profile":

[72] Using a Private ID Graph, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/IDManagement/private_id_setup.html [https://perma.cc/U2YD-F4T8].

[73] Joseph Cox, *Inside the Industry That Unmasks People at Scale*, Vice, (July 14, 2021), https://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii [https://perma.cc/TZ64-ECAG].

[74] *Oracle Buys Datalogix*, Oracle (Jan. 23, 2015), https://web.archive.org/web/20200807021726/https://www.oracle.com/us/corporate/acquisitions/datalogix/general-presentation-2395307.pdf [https://perma.cc/MQR4-5UEC].

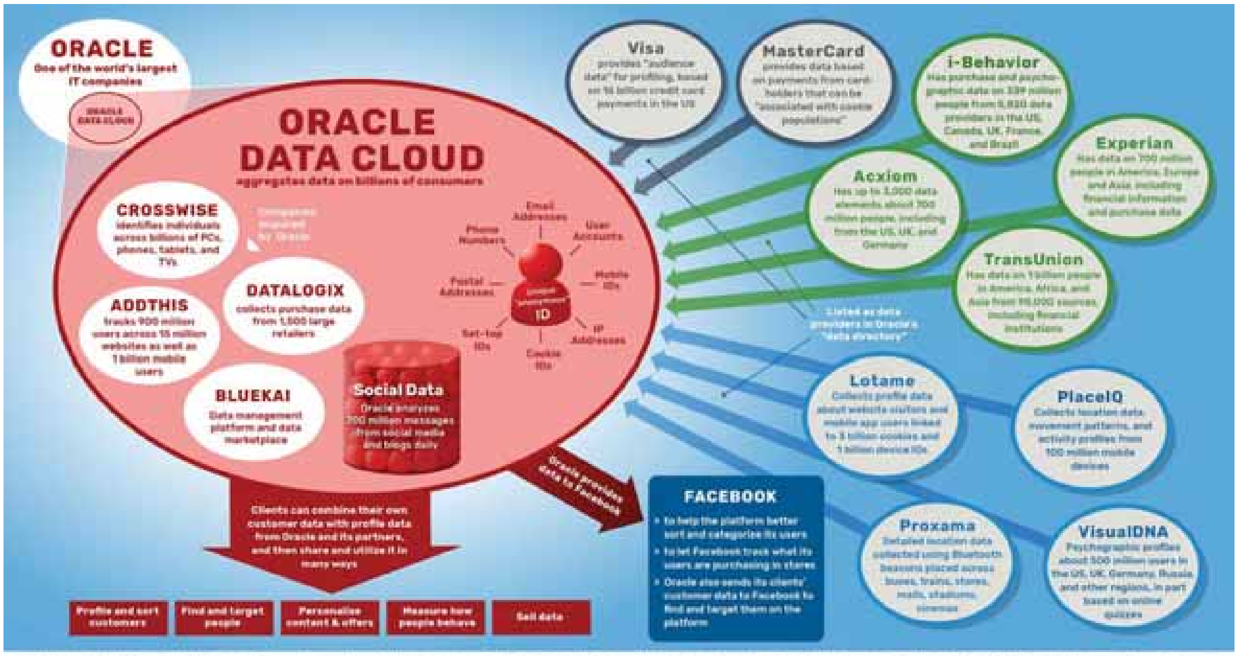


Oracle Identity Graph Unites All Interactions Across Various Channels to Create One Addressable Consumer Profile

- Identify customers and prospects everywhere
- Unify addressable identities across all devices, screens and channels
- Deliver a more relevant customer experience

67. A 2019 investigation into Oracle's profiling activities[75] resulted in the following analysis demonstrating the all-encompassing nature of the online and offline data Oracle collects and associates with IDs, which are tied to individual Class members, including information related to credit card purchases from Visa and MasterCard, brick-and-mortar establishments, and credit reporting agencies:

[75] Wolfie Christl, *Corporate Surveillance in Everyday Life*, Cracked Labs (Jun. 2017), https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf [https://perma.cc/T7Z6-JPZK].


ORACLE
One of the world's largest IT companies
ORACLE DATA CLOUD
ORACLE DATA CLOUD
aggregates data on billions of consumers
CROSSWISE
identifies individuals across billions of PCs, phones, tablets, and TVs
Companies acquired by Oracle
ADDTHIS
tracks 900 million users across 15 million websites as well as 1 billion mobile users
DATALOGIX
collects purchase data from 1,500 large retailers
BLUEKAI
Data management platform and data marketplace
Social Data
Oracle analyses 700 million messages from social media and blogs daily
Email Addresses
Phone Numbers
User Accounts
Postal Addresses
Mobile IDs
Unique consumer ID
Set-top IDs
Cookie IDs
IP Addresses
Clients can combine their own customer data with profile data from Oracle and its partners, and then share and utilize it in many ways
Profile and sort customers
Find and target people
Personalize content & offers
Measure how people behave
Sell data
Oracle provides data to Facebook
FACEBOOK
• to help the platform better sort and categorize its users
• to let Facebook track what its users are purchasing in stores
• Oracle also sends its clients' customer data to Facebook to find and target them on the platform
Visa
provides "audience data" for profiling, based on 16 billion credit card payments in the US
MasterCard
provides data based on payments from card-holders that can be "associated with cookie populations"
i-Behavior
Has purchase and psychographic data on 339 million people from 5,830 data providers in the US, Canada, UK, France, and Brazil
Acxiom
Has up to 3,000 data elements about 700 million people, including from the US, UK, and Germany
Experian
Has data on 700 million people in America, Europe and Asia, including financial information and purchase data
TransUnion
Has data on 1 billion people in America, Africa, and Asia from 90,000 sources, including financial institutions
Listed as data providers in Oracle's "data directory"
Lotame
Collects profile data about website visitors and mobile app users linked to 3 billion cookies and 1 billion device IDs
PlaceIQ
Collects location data, movement patterns, and activity profiles from 100 million mobile devices
Proxama
Detailed location data collected using Bluetooth beacons placed across buses, trains, stores, malls, stadiums, cinemas
VisualDNA
Psychographic profiles about 500 million users in the US, UK, Germany, Russia and other regions, in part based on online quizzes

© Cracked Labs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information, mainly the companies' own statements. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Oracle website, press releases, data directory brochures, presentations, MasterCard website, Acxiom annual report, TransUnion annual report, Lotame website, VisualDNA brochure, Facebook website, ProPublica article. For details about the sources see the report "Corporate Surveillance in Everyday Life".

68. In 2016, approximately one year after launch, Oracle Chairman and Chief Technological Officer Larry Ellison boasted there were five billion people in Oracle's ID Graph.[76]

69. According to Ellison, the purpose of Oracle ID Graph is to predict and influence the future behavior of billions of people. He explained Oracle could achieve this goal by looking at social activity and locations in real time, including "micro location[s]." For example, Ellison has represented that companies will be able to know how much time someone spends in a specific aisle of a specific store and what is in the aisle of the store. "By collecting this data and marrying it to things like micro location information, Internet users' search histories, websites visits and product comparisons along with their demographic data, and past purchase data, Oracle will be able to predict purchase intent better than anyone."[77]

70. Ellison likened the breadth and detail of Oracle's data collection to Facebook's—even arguing Oracle is better at mass surveillance and profiling than Facebook:

> Now where does this demographic data come from? Where does this past purchasing stuff come from? Well Oracle Data Cloud is the world's largest data

[76] Andrew Birmingham, *Oracle Has Five Billion Consumers In Its Identity Graph: Ellison*, Linkedin (Sept. 19, 2016) https://www.linkedin.com/pulse/oracle-has-five-billion-consumers-its-identity-graph-birmingham [https://perma.cc/MZ57-C4UN].

[77] *Id.*

> base. There are two big databases to keep track of consumers and which have a lot of information about consumers. One is very famous, it's called Facebook. The other one is less well known, it's Oracle's Data Cloud . . .They have great data, don't get me wrong. Facebook has incredible data assets, but so do we. In our data cloud marketers are able to target consumers and do a much better job at predicting what they're going to buy next.[78]

71. Ellison's vision for mass surveillance and profiling is totalizing and extends to the entire world: "How many people are on earth? Seven billion, two billion to go."[79]

C. <u>Oracle Uses the Data Marketplace to Enrich the Dossiers It Compiles on Class Members.</u>

72. Oracle, its partners, and its customers work in parallel to compile personal data and associate that data with specific individuals, effectively creating "dossiers" on people across the world. Oracle accomplishes its dossier building through its multifarious business practices, including not only the functionality of the Oracle ID Graph that connects, unifies, and then associates data to a person into a "profile," but also the functioning of the Oracle Data Marketplace. Oracle's Data Marketplace is an online store owned and operated by Oracle where Oracle facilitates the buying and selling of data and data-derived services by Oracle and its so-called "premier partners" to private, commercial, and governmental entities. The Data Marketplace allows the confluence of mass amounts of personal data by which its participants, including Oracle, can continually track people's activities and enrich people's dossiers.

73. The Data Marketplace trades in (1) personal data that Oracle collects itself such as that collected via BlueKai tracking pixels (first-party data); (2) personal data that private companies collect from their own users and sell directly to Oracle clients (second-party data); and (3) personal data that other third-party data brokers collect and sell to Oracle clients on the Data Marketplace (third-party data).

1. <u>Oracle Audiences.</u>

74. Oracle Audiences are derived from the raw personal information that Oracle itself collects from Internet users via the cookies, tracking pixels, cross-device tracking, AddThis, and

[78] *Id.*
[79] *Id.*

Datalogix technologies described above.[80] Oracle takes this personal information and applies algorithmic processing to develop inferences about specific people. Oracle uses the inferences it has made to assign people to certain "audiences" or segments.

75. For example, for Mother's Day, Oracle's marketing materials explained that Oracle's proprietary audience segments could help marketers target the following groups: (1) "Millennials spoil moms," 24-35 year olds who Oracle predicted were going to purchase higher priced gifts such as jewelry or electronics, (2) "Breakfast at Tiffany's," or people who were "more likely to spring for earrings over roses," and (3) "Mama's boys," 18-24 year old men who were likely going to buy an expensive gift for their mother.[81] Oracle touts that Oracle Audiences are effective because "the best predictor of future behavior is past behavior."

76. Oracle's Health and Wellness segments reveal sensitive, health-related types of personal information Oracle collects on Class members. By way of example only, these segments include individuals struggling with insomnia ("Sleeping aids"), acne ("Acne Treatments"), weight issues ("Diet Programs," "Weight Loss Programs," and "Adult Nutrition & Weight Control"), and nicotine addiction ("Smoking cessation").[82]

2. <u>Second-party data.</u>

77. Oracle also facilitates the sale and purchase of second-party data, i.e., personal information collected from Internet users by one company and sold directly to another company. Data buyers can browse the second-party data listings on the Data Marketplace and contact data sellers.[83] These direct deals occur in a closed, private market operated by Oracle: "The data seller,

[80] *Oracle Audiences*, Oracle, https://www.oracle.com/cx/advertising/audiences/ [https://perma.cc/C9TV-QUAW].

[81] *Give Your Mother's Day Campaigns the SpecialTtreatment*, Oracle, https://www.oracle.com/a/ocom/docs/cx-mothers-day-audience-data.pdf [https://perma.cc/8QBP-86NF].

[82] *Health and Wellness Preference Data Segments*, Oracle, https://www.oracle.com/us/assets/health-data-segments-020715-2537890.pdf [https://perma.cc/9FWJ-AUJM].

[83] *Using the Second-party Data Discovery Marketplace*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/ManagingTaxonomy/second-party_data_marketplace.html [https://perma.cc/464C-R426].

buyer, and Oracle can then work together to make a deal."[84] After purchase, buyers can enhance the ID Graph by uniting the second-party data with other personal information in the ID Graph, thereby painting a more specific and detailed picture of Internet users.

3. Other Data Brokers (Third-party data).

78. Oracle operates the world's largest third-party data marketplace.[85] Third-party data is information collected by companies that do not have a direct relationship with Internet users. Data brokers participating in Oracle's Data Marketplace freely portray themselves as able to defeat users' anti-tracking precautions, a pitch at odds with Oracle's privacy policies and its professed respect for the right of individuals to opt out. For instance, ALC Real World Data, a "branded data provider[] available through the BlueKai Marketplace" that offers "political" data, claims to provide "a deeper understanding of the people you're targeting" because it "has no cookies to erase and can't be 'cleared.'"[86]

79. Oracle partners with over 65 major brokers of third-party data and refers to these companies as "Branded Data Providers."[87] The personal information sold by Branded Data Providers on the Oracle Data Marketplace can be used to enhance the digital dossiers in the Oracle ID Graph.[88] A number of Oracle's Branded Data Providers sell highly intrusive and offensive personal information without consent:

a. Mobilewalla: Boasts of having "billions of data points daily" from 276 million unique mobile devices in the U.S. alone[89], and 1.5 billion mobile devices in 31 countries

[84] *Id.*

[85] *Oracle Data Marketplace*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/AudienceDataMarketplace/AudienceDataMarketplace.html [https://perma.cc/27S8-GX7H].

[86] *2019 Data Directory*, Oracle (2019), https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf [https://perma.cc/EV8L-PG7V].

[87] *Branded Data Providers*, Oracle, https://www.oracle.com/cx/advertising/data-providers/ [https://perma.cc/7VBG-34XD].

[88] *Get o the Heart of the Matter, the Heart of Your Customer*, Oracle, https://www.oracle.com/assets/brochure-data-driven-marketing-odc-2894231.pdf [https://perma.cc/3W3X-JYC7].

[89] *Warren, Maloney, Wyden, DeSaulnier Probe Data Broker's Collection of Data on Black Lives Matter Demonstrators*, House Committee on Oversight and Reform, Chairwoman Carolyn B.

worldwide.[90] In particular, Mobilewalla sells age, gender, GPS, and location data. Mobilewalla specifically advertises the personal location information it sells as a way to increase political campaign results.[91] During the summer of 2020, Mobilewalla tracked mobile devices to collect data on 17,000 Black Lives Matter protesters including their home addresses and demographics. Mobilewalla also released a report entitled "George Floyd Protester Demographics: Insights Across 4 Major US Cities," which prompted a letter and investigation by Senator Elizabeth Warren and other congress members.[92] In response to this investigation, Mobilewalla revealed that it had provided location data used by the Department of Homeland Security, the Internal Revenue Service, and the U.S. military for warrantless tracking of devices both at home and abroad.[93]

b. 140 Proof: Collects data from 700-plus million social media users across various social networks. The data includes content as well as meta-data such as "follows, check-ins, re-blogs, pins, likes, or share." It claims to be able to build and target audiences for "hard to find users" and "social influencers."[94]

c. Affinity Answers: Advertises data on Class members' interests in political organizations (e.g., NAACP, National LGBTQ Task Force, Planned Parenthood), political media figures (e.g., Bill O'Reilly, Glenn Beck, Anderson Cooper, Arianna Huffington), state-level

Maloney, (Aug. 4, 2020) https://oversight.house.gov/news/press-releases/warren-maloney-wyden-desaulnier-probe-data-brokers-collection-of-data-on-black [https://perma.cc/VKW2-NQSK].

[90] *What is Geo-Behavioral Advertising?*, Mobilwalla (Feb. 8, 2019), https://www.mobilewalla.com/blog/what-is-geo-behavioral-advertising [https://perma.cc/N9H2-YTRC].

[91] *Audience Segments*, Mobilewalla, https://www.mobilewalla.com/products/audience-segments [https://perma.cc/KW4D-H5F7].

[92] John Donegan, *The Incessant Surveillance by Data Brokers Needs to be Addressed*, ManageEngine (Oct. 6, 2021), https://insights.manageengine.com/privacy-compliance/the-incessant-surveillance-by-data-brokers-needs-to-be-addressed/ [https://perma.cc/F8HX-ZPHF].

[93] Bryan Tau, *How Cellphone Data Collected for Advertizing Landed at U.S. Government Agencies*, The Wall Street Journal (November 18, 2021, 8:30 AM ET), https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-ended-up-with-government-11637242202 [https://perma.cc/S6AB-93XY].

[94] *Oracle Data Cloud Data Directory*, Oracle, https://web.archive.org/web/20180501185159/http://oracle.com/us/solutions/cloud/data-directory-2810741.pdf [https://perma.cc/ANG8-H277].

Democratic Party and Republican Party organizations, and specific politicians in office.[95] It harvests information about hundreds of millions of users from major social networks such as Facebook, Instagram, and Twitter.

d. Gravy Analytics: Advertises location intelligence at "millions of places, points-of-interest and local events" to power "precision-targeted mobile advertising campaigns." Its "Brand Audiences" include 2000-plus U.S. chain locations such as BestBuy, Burger King, Starbucks, and Target.[96] It also sells phone location data to government agencies.[97] Indeed, the FBI contracts with Gravy Analytics' subsidiary, Venntel, for the monitoring of social media posts and location data. In 2020, the House Committee on Oversight and Reform opened an investigation into Venntel for its business of buying location data from various smartphone apps and selling that data to agencies including the FBI, Department of Homeland Security, DEA, ICE, CBP, and the IRS. The Trump Administration also used Gravy Analytics' location data to track people crossing the US-Mexico border.

e. Acxiom: This massive data broker openly and explicitly advertises that it has data on 45.5 million current and former U.S. military personnel.[98]

[95] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, Duke University Sanford Cyber Policy Program (2021), https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf [https://perma.cc/34SV-XY6M].

[96] *Gravy Analytics Unveils Location Data Forensics*, Gravy Analytics (Dec. 19, 2018), https://gravyanalytics.com/press/gravy-analytics-unveils-location-data-forensics/ [https://perma.cc/SE3K-KMSH]; *Location-Based Advertising: Brand Audiences*, Gravy Analytics (Mar. 26, 2018), https://gravyanalytics.com/blog/location-based-advertising-branded-audiences/ [https://perma.cc/4C4B-PSYP]; *Paramount, Best Buy & Gravy Analytics: Consumer Insights for Advertising*, Gravy Analytics, https://gravyanalytics.com/paramount-best-buy/ [https://perma.cc/E8UU-H6AY] ; *Starbucks & the Pumpkin Spice Latte: Using Location Data to Measure Foot Traffic*, Gravy Analytics, (Aug. 21, 2019), https://gravyanalytics.com/blog/starbucks-the-pumpkin-spice-latte-using-location-data-to-measure-foot-traffic/ [https://perma.cc/9PVQ-ME55].

[97] Lee Fang, *FBI Expands Ability To Collect Cellphone Location Data, Monitor Social Media, Recent Contracts Show*, The Intercept (Jun. 24, 2020, 11:56 AM), https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/ [https://perma.cc/MJ58-QL3Z].

[98] Justin Sherman, *Data Brokers Are Advertising Data on U.S. Military Personnel*, Lawfare (Aug. 23, 2021), https://www.lawfareblog.com/data-brokers-are-advertising-data-us-military-personnel [https://perma.cc/LHP5-ZK2G].

80. Oracle provides, and profits from, this data marketplace that allows third-party data brokers to traffic in Class members' highly sensitive personal information. The following examples non-exhaustively illustrate the types of sensitive information Oracle facilitates the sale of in its marketplace:

a. *Race*: At least five data brokers expressly provide racial categories as "audience segments." These include "African American," "Asian," "Hispanic," "Caucasian," and "American Indian."[99] Multiple data brokers' (e.g., Retargetly, DataXpand) business model consists entirely of targeting Hispanic audiences.[100]

b. *Location*: Data brokers offer location tracking, including a "real-time GPS signal." Mobilewalla, for instance, described above, has advertised to Oracle customers that its data can be used to serve a person an ad "at a specific time (say between 8-8:30PM), at a specific location/place (say at the AT&T Stadium in Dallas) during a specific event (say, a country music concert by Shania Twain)."[101] Cuebiq advertises "precise location data" from 61+ million U.S. smartphone users on over 180 mobile apps.[102] TrueData advertisers "real-time GPS and beacon location signals" on 245 million U.S. mobile users.[103]

c. *Politics*: Data brokers participating in Oracle's Data Marketplace purport to offer segments based on detailed political information, and some are avowedly partisan in doing so. i360, for example, bills itself as "the leading data and technology resource for the pro-free-market political and advocacy community" with a database of "199 million voters from all 50

[99] *2019 Data Directory*, Oracle (2019), https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf [https://perma.cc/EV8L-PG7V].

[100] *Helping You Understand and Reach Latin American Consumers Through Digital*, Retargetly, https://retargetly.com/ [https://perma.cc/PS4C-JQR9].

[101] Anindya Datta, *A largely Ignored But Critical Dimension to Incorporate in Understanding Consumers on Mobile. The Data Source, Inspired Thinking on our Data-Driven World.* Oracle (Fall 2016), https://cdn2.hubspot.net/hubfs/4309344/the-data-source-magazine-fall-2016.pdf [https://perma.cc/ZZ8S-5RBK].

[102] *Cuebiq and Drawbridge Double-Down on Cross-Device Reach & Attribution*. Cuebiq. https://www.cuebiq.com/press/cuebiq-drawbridge-reach-attribution/ [https://perma.cc/GK4T-V8FX].

[103] *Holiday Campaign Planner: 3 Critical Strategies to (Re)Connect to Retail Mobile Customers*, TrueData, https://www.truedata.co/holiday-campaign-planner-3-critical-strategies-to-reconnect-to-retail-mobile-customers/ [https://perma.cc/8ALU-6DHZ].

states."[104] It boasts a dataset that includes "extensive political identification, coalition and membership information collected by way of in-person, phone and online surveys, as well as through partner relationships in addition to lifestyle and consumer data collected from multiple top-tier providers."[105] It advertises registration and partisanship segments such as "Catholic," "Pro 2nd Amendment," "Pro Choice," "Pro Life," "Pro Marriage Same Sex," "Pro Traditional Marriage," "Democratic Voters," "Independent Voters," "Republican Voters," "Swing Dem Voters," and "Swing GOP Voters."[106]

d. *Medical*: OnAudience, a "data provider" that profiles Internet users by "observing user activity based on websites visited, content consumed and history paths to find clear behavior patterns and proper level of intent,"[107] lets customers target individuals categorized as interested in "Brain Tumor," "AIDS & HIV," "Substance Abuse" and "Incest & Abuse Support."[108]

81. Oracle monetizes Class members' personal information in part by providing a process through which Oracle clients can winnow Oracle's vast store of detailed user data into fine-grained audiences. For instance, an Oracle client could choose to filter billions of people down to a handful of Class members who fit a cross-section of micro-targeted segments. Oracle also allows clients to create audiences that exclude based on any or all of the same criteria.

[104] *comScore and i360 Team Up to Provide Digital Marketing Insights for Political Campaigns and Advocacy Groups*, Cision PR Newsire (Apr. 17, 2012), https://www.prnewswire.com/news-releases/comscore-and-i360-team-up-to-provide-digital-marketing-insights-for-political-campaigns-and-advocacy-groups-147750205.html [https://perma.cc/4F88-VHPT]; *The Database, Individual-Centric Data Warehouse*, i-360, https://www.i-360.com/the-database/ [https://perma.cc/8TY2-C9HH].

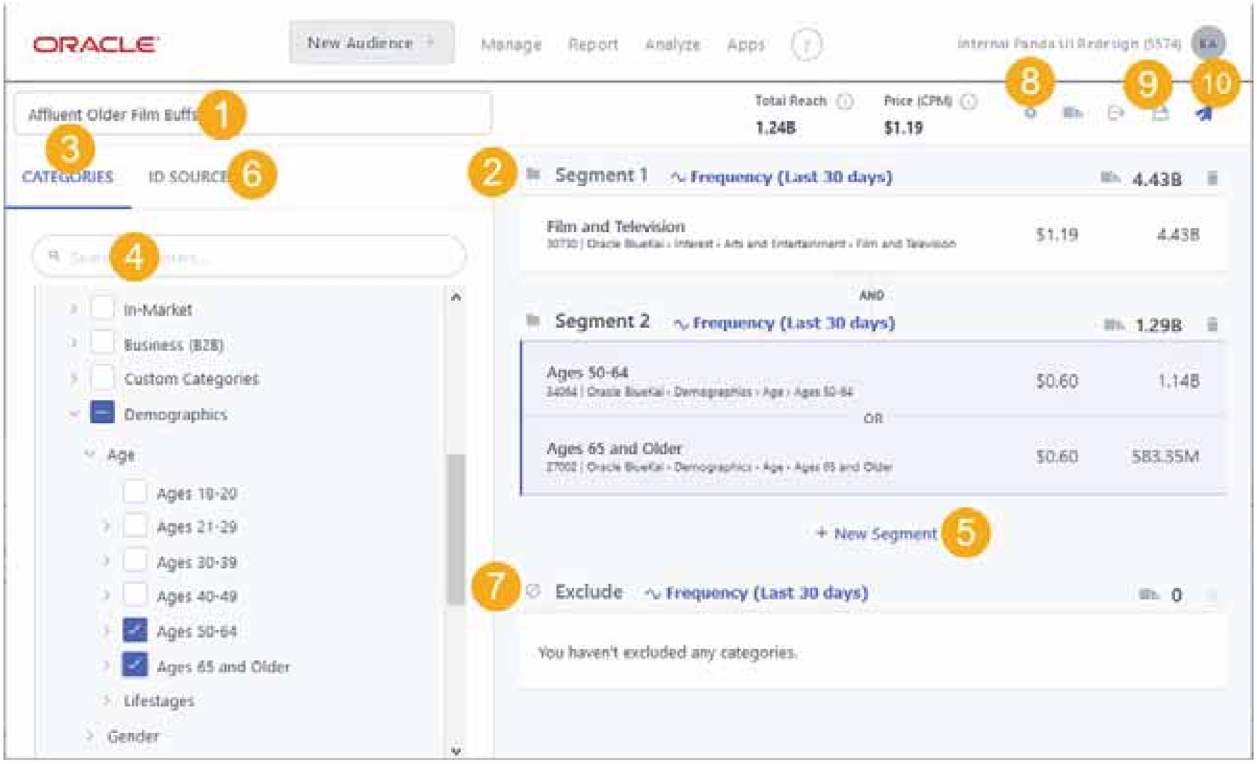
[105] *The Database, Individual-Centric Data Warehouse*, i-360, https://www.i-360.com/the-database/ [https://perma.cc/8TY2-C9HH].

[106] *Data Dictionary, Online Segments*, I-360, https://www.i-360.com/wp-content/uploads/2019/03/i360-Online-Segment-Data-Dictionary.pdf [https://perma.cc/392Q-3RFL].

[107] *2019 Data Directory*, Oracle (2019), https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf [https://perma.cc/EV8L-PG7V].

[108] Dr. Johnny Ryan, *Submission to the Irish Data Protection Commission*, Irish Council for Civil Liberties (Sept. 21, 2020), https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf [https://perma.cc/Y2J6-Z9YF].

82. Based on Oracle's public-facing documentation, Oracle provides detailed "control panels" to its clients which allows the clients to analyze, segment, and target Plaintiffs and Class members based on the digital dossiers Oracle has compiled on them[109]:



Affluent Older Film Buffs

Total Reach 1.24B

Price (CPM) $1.19

☐ In-Market
☐ Business (B2B)
☐ Custom Categories
▬ Demographics
Age
☐ Ages 18-20
☐ Ages 21-29
☐ Ages 30-39
☐ Ages 40-49
☑ Ages 50-64
☑ Ages 65 and Older
Lifestages
Gender

Segment 1 Frequency (Last 30 days) 4.43B

Film and Television 30730 | Oracle BlueKai › Interest › Arts and Entertainment › Film and Television	$1.19	4.43B

AND

Segment 2 Frequency (Last 30 days) 1.29B

Ages 50-64 34064 | Oracle BlueKai › Demographics › Age › Ages 50-64	$0.60	1.14B
OR		
Ages 65 and Older 27002 | Oracle BlueKai › Demographics › Age › Ages 65 and Older	$0.60	583.35M

Exclude Frequency (Last 30 days) 0

You haven't excluded any categories.

83. In other words, Oracle facilitates the creation of proxies for protected classes like race, and allows its clients to exclude on that basis. For example, one Oracle customer website describes how, after Facebook made it more difficult to target ads based on race in the employment and credit areas, Oracle helped it achieve the same result.[110]

84. Oracle clients include not only businesses looking to advertise their wares, but also political campaigns and government agencies seeking to surveil, investigate, or target particular individuals with propaganda. Oracle markets directly to these public agencies and political parties, and refers to them as "Public Sector Customers."

[109] *Creating Audiences*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/Audiences/create_audience.html [https://perma.cc/K6F2-NPZF].

[110] *Natural Intelligence Secures Higher Quality Purchases Using Oracle Audiences Within Skai*™, Skai, https://skai.io/case-studies/natural-intelligence-secures-higher-quality-purchases-using-s-third-party-audiences/ [https://perma.cc/UT5C-VQTU].

85. Political campaigns now have "needle-in-the-haystack capabilities" to "microtarget voters on all their devices" using personal information sold by data brokers.[111] The Trump campaign, for example, built a 220 million–person database of voter information named "Project Alamo" using Datalogix, a data collection platform owned by Oracle.[112] Project Alamo, powered by Oracle data, facilitated the Trump campaign's voter suppression initiatives including highly targeted political advertising to African Americans, white women, and young white liberals[113] in 16 swing states, several of which were narrowly won by Trump. In Michigan, a state that Trump won by only 10,000 votes, 15% of voters are black, but they represented 33% of Project Alamo's "special deterrence" category.[114] These voters received anti-Clinton Facebook ads that included audio of Hilary Clinton referring to African-American children as "superpredators."[115] Through Project Alamo's voter suppression efforts, it is estimated that 2 million black voters who voted in 2012 did not vote in 2016.[116]

86. Oracle also powers "Facebook Custom Audiences" which allows advertisers, including political parties and campaigns around the world, to push ads to Facebook using personal data unlawfully collected and sold by Oracle.[117] Oracle also recently announced a

[111] Jeff Chester, *Our Next President: Also Brought to You by Big Data and Digital Advertising*, Bill Moyers (Jan. 6, 2017), https://billmoyers.com/story/our-next-president-also-brought-to-you-by-big-data-and-digital-advertising/ [https://perma.cc/R8FE-9J9W].

[112] Nina Burleigh, *How Big Data Mines Personal Info to Craft Fake News and Manipulate Voters*, Newsweek (Jun. 8, 2017, 1:01 PM), https://www.newsweek.com/2017/06/16/big-data-mines-personal-info-manipulate-voters-623131.html [https://perma.cc/6DZ4-WYD9].

[113] Joshua Green & Sasha Issenberg, *Inside the Trump Bunker, With Only Days to Go*, Bloomberg (Oct. 27, 2016, 3:00 AM PDT), https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go [https://perma.cc/9RN2-WCKS].

[114] Dan Sabbagh, *Trump 2016 Campaign 'Targeted 3.5m Black Americans to Deter them From Voting'*, The Guardian, (Sept. 28, 2020, 1:24 PM EDT), https://www.theguardian.com/us-news/2020/sep/28/trump-2016-campaign-targeted-35m-black-americans-to-deter-them-from-voting [https://perma.cc/W4GX-UHTN].

[115] Andrew Marantz, *The Man Behind Trump's Facebook Juggernaut*, The New Yorker (Mar. 2, 2020), https://www.newyorker.com/magazine/2020/03/09/the-man-behind-trumps-facebook-juggernaut [https://perma.cc/TE8H-DTR5].

[116] Dan Sabbagh, *Trump 2016 Campaign 'Targeted 3.5m Black Americans to Deter them From Voting'*, The Guardian, (Sept. 28, 2020, 1:24 PM EDT), https://www.theguardian.com/us-news/2020/sep/28/trump-2016-campaign-targeted-35m-black-americans-to-deter-them-from-voting [https://perma.cc/W4GX-UHTN].

[117] *Find Buyers at Scale on Facebook With Oracle Data*, Oracle, https://www.oracle.com/a/ocom/docs/six-steps-activating-odc-audiences-on-facebook.pdf

partnership with Amazon: Oracle Audiences is now integrated into the Amazon platform allowing Oracle's clients to target Amazon users.[118]

87. The general public does not have access to the Data Marketplace, or any visibility into who is buying and selling their information. Access is restricted to buyers and sellers, so individuals whose data is being bought and sold have no reasonable insight into what occurs there or the extent of Oracle's violations of their privacy rights. Publicly available information indicates that data sold on the Data Marketplace is highly sensitive, and is collected in pernicious and illegal ways.

88. Oracle does not publicly disclose the identity of its clients that participate on the Data Marketplace. Plaintiffs and Class members have no reasonable basis to discern the identity of the persons and/or entities that buy or sell information about them on the Data Marketplace.[119] This opacity extends to possible state actors. Oracle has a well-documented history of marketing its technology to state actors within the United States and abroad.[120] While Oracle *does* have a total embargo on data sales to a small group of countries including Iran, North Korea, and Syria,[121] it has marketed its surveillance products to governments, police or paramilitary forces, including

[https://perma.cc/G7R5-5CJM].

[118] Rob Tarkoff, *Oracle and Amazon Advertising Help Advertisers Engage Online Shoppers*, Oracle Blog (Jun. 2, 2021), https://www.oracle.com/news/announcement/blog/oracle-amazon-advertising-help-advertisers-engage-shoppers-2021-06-02/ [https://perma.cc/L864-A2EA].

[119] Nor, for that matter, does Oracle disclose what process it uses to vet Data Marketplace participants.

[120] *Government and Education*, Oracle, https://www.oracle.com/industries/government/ [https://perma.cc/J5NN-E97U].

[121] *Data Restrictions*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Introduction/Privacy/embargo.html [https://perma.cc/NQ83-FJUP].

China,[122] Brazil, Mexico, Pakistan, and the United Arab Emirates.[123]

D. Data Brokers Are a Recognized Threat to Individual Privacy.

89. The California Consumer Privacy Act (CCPA) defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80. The CCPA requires a data broker to register with the Attorney General. Oracle is registered as data broker in California pursuant to the CCPA.

90. The New York Times has described data brokers as "Big Brother-in-Law,"[124] noting that the copious information they compile on individuals is "fused and vetted by algorithm to form an ever-evolving, 360-degree view of U.S. residents' lives."[125] As described in the Financial Times, "[t]he explosive growth of online data has led to the emergence of the super data broker —*the 'privacy deathstars', such as Oracle* . . . that provide one-stop shopping for hundreds of different data points which can be added into a single person's file . . . As a result, everyone now is invisibly attached to a living, breathing database that tracks their every move."[126]

91. Legislators have recognized the privacy-invasive nature of data brokers' core business practices. The sale of Americans' information to foreign states is a source of increasing

[122] Mara Hvistendahl, *How Oracle Sells Repression in China*, The Intercept (Feb. 18, 2021, 3:20 AM), https://theintercept.com/2021/02/18/oracle-china-police-surveillance/ [https://perma.cc/W45L-RGTE]; Mara Hvistendahl, *How a Chinese Surveillance Broker Became Oracle's "Partner of the Year"*, The Intercept (Apr. 22, 2021, 12:00 AM) https://theintercept.com/2021/04/22/oracle-digital-china-resellers-brokers-surveillance/ [https://perma.cc/RXJ6-38VD]; Mara Hvistendahl, *Oracle Executive's Contentious Interview with the Reporter He Sought Dirt On*, The Intercept (Apr. 30, 2021, 10:06 AM), https://theintercept.com/2021/04/30/oracle-china-ken-glueck/ [https://perma.cc/Z9VW-QZAW]; Mara Hvistendahl, *Oracle Boasted That its Software Was Used Against U.S. Protesters. Then It Took the Tech to China*, The Intercept (May 25, 2021, 8:25 AM), https://theintercept.com/2021/05/25/oracle-social-media-surveillance-protests-endeca/ [https://perma.cc/9RXG-CF5M].

[123] Mara Hvistendahl, *How a Chinese Surveillance Broker Became Oracle's "Partner of the Year"*, The Intercept (Apr. 22, 2021, 12:00 AM), https://theintercept.com/2021/04/22/oracle-digital-china-resellers-brokers-surveillance/ [https://perma.cc/RXJ6-38VD].

[124] McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age*, The New York Times Magazine (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html [https://perma.cc/5678-ZEJX].

[125] *Id.*

[126] Aliya Ram & Madhumita Murgia, *Data Brokers: Regulators try to Rein in the "Privacy Deathstars"*, Financial Times (Jan. 8, 2019), ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521 [https://perma.cc/36DS-3R72] (emphasis added).

public concern. Senator Ron Wyden, for example, has cited fears about the sale of location data, credit card purchases, and web browsing to the People's Republic of China as the impetus for a bill—the Protecting Americans' Data From Foreign Surveillance Act—that would largely bar the export of Americans' personal data.[127]

92. Senator Wyden has also introduced the "Fourth Amendment is Not for Sale Act" to "put a stop to shady data brokers buying and selling Americans' Constitutional rights." The proposed Act "closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement and intelligence agencies without any court oversight – in contrast to the strict rules for phone companies, social media sites and other businesses that have direct relationships with consumers." As Senator Wyden explained:

> Doing business online doesn't amount to giving the government permission to track your every movement or rifle through the most personal details of your life … There's no reason information scavenged by data brokers should be treated differently than the same data held by your phone company or email provider. This bill closes that legal loophole and ensures that the government can't use its credit card to end-run the Fourth Amendment.[128]

93. On December 8, 2021, Senator Wyden, in urging the Consumer Financial Protection Bureau to take action against data brokers, stated:

> Data brokers are serving as shady middlemen to sell [consumers'] personal information without any legal protections . . . Selling personal information that people provide to sign up for power, water and other necessities of life, and giving them no choice in the matter, is an egregious abuse of consumers' privacy.[129]

94. The FTC has recently warned consumers about the "shadowy" "data broker ecosystem" where "companies have a profit motive to share data at an unprecedented scale and

[127] *The Protecting Americans' Data From Foreign Surveillance Act*, Ron Wyden, United States Senator for Oregon, https://www.wyden.senate.gov/imo/media/doc/Protecting%20Americans%20Data%20from%20Foreign%20Surveillance%20Act%20of%202021%20One%20Pager.pdf [https://perma.cc/FS24-9XEB].

[128] *Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act*, Ron Wyden, United States Senator for Oregon (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act- [https://perma.cc/LMP7-CWFU].

[129] *Wyden Urges CFPB to Protect Americans' Privacy and Stop the Sale of Personal Data by Credit Agencies*, Ron Wyden, United States Senator for Oregon, https://www.wyden.senate.gov/news/press-releases/wyden-urges-cfpb-to-protect-americans-privacy-and-stop-the-sale-of-personal-data-by-credit-agencies [https://perma.cc/N777-6US8].

granularity," including a "staggering" amount of "highly personal information that people choose not to disclose even to family, friends, or colleagues."[130]

95. In the wake of *Dobbs v. Jackson Women's Health Organizatio*n, No. 19-1392, 142 S. Ct. 2228 (2022), the threat data brokers like Oracle pose to the privacy of individuals seeking information about abortions is significantly magnified. An investigation recently revealed Oracle trackers on the websites of nonprofits providing abortion resources and services, including Planned Parenthood.[131] Class members who have visited Planned Parenthood's website in states where abortion is now illegal may have had their personal information tracked and compiled by Oracle, which Oracle may then make available to law enforcement officials.

96. Congressional representatives have expressed intense concern about law enforcement officials using Oracle data to surveil and prosecute individuals researching abortion. House Democrats recently sent Oracle a letter asking it to limit its sale of sensitive location data.[132] Senators Elizabeth Warren and Wyden have also introduced the "Health and Location Data Protection Act," which would ban data brokers like Oracle from selling health and location data. As Senators Warren and Wyden state:

> Data brokers profit from the location data of millions of people, posing serious risks to Americans everywhere by selling their most private information . . . [w]hen abortion is illegal, researching reproductive health care online, updating a period-tracking app, or bringing a phone to the doctor's office all could be used to track and prosecute women across the U.S. It amounts to uterus surveillance.[133]

[130] Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the law Against Illegal Use and Sharing of Highly Sensitive Data*, The Federal Trade Commission (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use [https://perma.cc/V6XT-85YX].

[131] Alfred Ng & Maddy Varner, *Nonprofit Websites are Riddled with Ad* Trackers, The Markup (Oct. 21, 2021, 8:00 AM ET), https://themarkup.org/blacklight/2021/10/21/nonprofit-websites-are-riddled-with-ad-trackers [https://perma.cc/PW23-K5F2].

[132] Cristiano Lima, *Democrats Press Oracle, AWS Over Their Post-Roe Data Collection*, The Washington Post (July 21, 2022), https://www.washingtonpost.com/politics/2022/07/21/democrats-press-oracle-aws-over-their-post-roe-data-collection/ [https://perma.cc/M4S9-CGDM].

[133] *Warren, Wyden, Murray, Whitehouse, Sanders Introduce Legislation to Ban Data Brokers from Selling Americans' Location and Health Data*, Elizabeth Warren, United States Senator for Massachusetts (June 15, 2022), https://www.warren.senate.gov/newsroom/press-releases/warren-wyden-murray-whitehouse-sanders-introduce-legislation-to-ban-data-brokers-from-selling-americans-location-and-health-data [https://perma.cc/J5XV-JFSR].

97. Consistent with Oracle's plan of engaging in wide-ranging surveillance of the intimate health details of all Americans, Oracle's Larry Ellison has announced Oracle's plan to build "a unified national health records database," which it is effectuating through its $28.3 billion acquisition of electronic health record company Cerners. According to Ellison, Oracle is "building a system where the health records [of] all American citizens[] . . . not only exist at the hospital level but also are in a unified national health records database," apparently to be maintained and controlled by Oracle.[134] Oracle plans to build this massive health database *prior to even purporting to obtain consent from patients:* "Ellison said this new system will only have anonymous information *until individual patients give consent*."[135]

98. Oracle has *itself* acknowledged the highly problematic nature of its own profile-building conduct, albeit indirectly. Without a trace of irony, Oracle has argued to legislators both in the U.S. and internationally that its business rival Google wrongfully builds "shadow profiles," "using massive amounts of consumer data, not all of which it discloses to consumers, to micro-targe[t] advertising" to consumers without their consent. However, Oracle's description of Google's conduct is a virtually word-for-word description of its own conduct as a data broker. According to Oracle, Google's "shadow profiles" are:

> [M]assive, largely hidden datasets of online and offline activities. This information is collected through an extensive web of Google [*cf*. Oracle] services, which is difficult, if not impossible to avoid. *It is largely collected invisibly and without consumer consent.* Processed by algorithms and artificial intelligence, this data reveals an intimate picture of a specific consumer's movements, socio-economics, demographics, "likes," activities and more. It may or may not be associated with a specific users' name, but the specificity of this information defines the individual in such detail that a name is unnecessary.[136]

[134] Heather Landi, *Oracle, Cerner Plan to Build National Medical Records Database as Larry Ellison Pitches Bold Visionfor Healthcare*, Fierce Healthcare (June 10, 2022, 6:22 AM) https://www.fiercehealthcare.com/health-tech/oracle-cerner-plan-build-national-medical-records-database-ellison-pitches-bold-vision [https://perma.cc/G44G-77L6].

[135] Brody Ford, *Oracle's Ellison Pitches US Health Database With Power of Cerner*, Bloomberg (June 9, 2022, 2:35 PM PDT), https://www.bloomberg.com/news/articles/2022-06-09/oracle-s-ellison-pitches-national-health-database-on-cerner-deal [https://perma.cc/QB47-HYRG] (emphasis added).

[136] *Oracle Corporation Submission to the Digital Platforms Inquiry*, Oracle, https://www.accc.gov.au/system/files/Oracle%20Corporation%20%28March%202019%29.PDF [https://perma.cc/LHE4-B47C].

The hypocrisy of Oracle's lobbying efforts on this front has been noted by commentators in the press.[137]

E. Class Members Have Not and Cannot Consent to Oracle's Collection or Use of their Personal Information.

99. The long-established common law, statutory, and Constitutional rights to privacy are inherently and inextricably linked to fundamental cultural values of autonomy and freedom. The concept of "consent" reinforces these cultural values by functioning as a way for individuals to protect their privacy by exercising control over their personal information—what personal information organizations can collect, how they can use it, and to whom they can disclose it. Oracle conducts the business practices alleged in this complaint within a context and in a manner where consent from the persons whose data it assembles is not reasonably possible or practical, in fact does not occur, and which in light of the extent of the privacy rights that are violated by Oracle's business practices, no consent to such practices could be enforced as a matter of law.

100. Plaintiffs and Class members, like our society at large, do not have the practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet, with their personal data traveling through cyberspace every day. Because much of daily activities of life are now conducted online—whether financial, commercial, or social—Internet activity has become an "exhaustive chronicle" of one's life. The personal data necessary for these activities courses through the Internet as these activities take place, and, when aggregated, can provide deep insight into a person's thinking, acting, and being. Without an expectation of privacy on the Internet, there would functionally be no expectation of privacy anywhere.

101. Oracle sits atop a complex data collection and processing apparatus feeding its labyrinthine multinational data marketplace, making it impossible for ordinary persons to reasonably understand the true purpose and extent of Oracle's data collection, compiling of digital dossiers, and other data exploitation practices, which are opaque, if not invisible, to ordinary data

[137] Mike Masnick, *Oracle's Projection: As It Accuses Google on Snooping on You, It Has Built a Huge Data Operation That it Doesn't Want Regulated*, techdirt (Apr. 9, 2021, 9:37 AM) https://www.techdirt.com/2021/04/09/oracles-projection-as-it-accuses-google-snooping-you-it-has-built-huge-data-operation-that-it-doesnt-want-regulated/ [https://perma.cc/X8WZ-ZUWJ] (emphasis added).

subjects. Given the complexity and disguised nature of Oracle's collection and use of personal information, and the lack of any direct relationship between Oracle and the Plaintiffs and Class members, there is no reasonable basis for Plaintiffs and the Class members to know the extent to which Oracle is obtaining their data, tracking them, and selling their data or services derived from their data.

102. Oracle's presence on the Internet and in the digital world is ubiquitous, by design, and its data gathering activities are constant, vast, and encompasses a massive swath of Internet activity. The breadth and complexity of sources from which Oracle compiles digital dossiers, or profiles, on Class members, including from credit card transactions and interactions with brick-and-mortar establishments, is such that as a practical matter, Plaintiffs and Class members have no way of knowing—and thus no way of even being able to consent to—the actual scope of Oracle's conduct. Plaintiffs and Class members, do not, merely by virtue of conducting the necessary activities of daily life, both online and in the physical world, consent to constant and pervasive surveillance by Oracle and the creation of detailed dossiers about them.

103. In as much as the Internet and digital existence has become integral to people's lives, its functioning and complexity with respect to personal data remains opaque to reasonably informed people. The Findings and Declarations of the California Privacy Rights Act (CPRA) notes that the "asymmetry of information" inherent in the "collect[ion] and use [of] consumers' personal information . . . makes it difficult for consumers to understand what they are exchanging and therefore to negotiate effectively with businesses." There is asymmetry of knowledge between Oracle and the data subjects it exploits, including Plaintiffs and the members of the Class, in that Oracle has an complete knowledge of its data collection and data exploitation practices, but Plaintiffs and Class members have no direct relationship with Oracle regarding these practices and no reasonable basis to discern those practices nor the nature of the practices directed at them.

104. Plaintiffs and Class members cannot reasonably foresee all the ways in which Oracle may use the detailed dossiers it is compiling on them. Plaintiffs and Class members have no way of knowing the specific third parties to which Oracle will provide their personal information, or what those third parties will do with that information. Plaintiffs and Class

members thus cannot provide knowing and informed consent to Oracle's dissemination of their personal information.

105. Oracle makes no pretense of having directly obtained consent from the persons whose data it gathers, including Plaintiffs and the Class members. At no point during its process of collecting or processing personal data, or the compiling of dossiers or selling services based on that personal data, does Oracle ever directly ask individuals for their consent. Oracle legally acknowledges this by virtue of its registration as a data broker wherein it admits it "does not have a direct relationship" with the subjects whose data it exploits. *See* Cal. Civ. Code § 1798.99.80.

106. Nor have Plaintiffs and the Class members manifested any form of consent indirectly to Oracle. Oracle publishes so-called privacy policies on its website, but these policies are not reasonably directed to Plaintiffs and Class members, all of whom lack any direct relationship with Oracle and have no reasonable insight into Oracle's data collection and data exploitation practices or how they may or may not be subject to such practices, and therefore there is no reasonable basis for Plaintiffs and Class members to be aware of Oracle's privacy policies or to have directed themselves to them. Plaintiffs and the Class members are not legally subject to or governed by Oracle's published privacy policies.

107. Oracle's so-called privacy policies are themselves insufficient to adequately inform Plaintiffs and the Class members about the nature and extent of Oracle's data collection and data exploitation practices, even with regard to their personal data. Plaintiffs and the Class members are in the course of daily life barraged with thousands of pages of purported "terms and conditions" and "privacy policies" for online products and services. Computer science researchers have estimated that, based on the number of unique sites American Internet users visit annually, it would take the average Internet user between 181 to 304 hours to read the relevant privacy policies; this translates to approximately 72 billion hours per year for every U.S. Internet user to read all the privacy policies he or she encounters. Oracle knows, or reasonably should know, that it is not reasonably possible for Internet users to read or comprehend the thousands of privacy policies they encounter, including Oracle's privacy policies.

108. As privacy scholars have noted, issues that users must navigate to understand the significance of consent are too complex and the conditions surrounding consent too easy to manipulate for any purported consent to be informed and meaningful.[138] While, as is well-known, many websites include "cookie popups" that purport to ask for consent for the website placing a cookie on the users' computer, in practice, most formulations of user control rights fail to sufficiently explain that cookies tracking leads to *profiling* based on information *derived* from user behavior. These practices, whether by Oracle or other third parties, fail to provide sufficient means to obtain the legally viable consent to Oracle's mass data collection, behavior tracking, and assembling of dossiers based on that data.

109. The content and organization of Oracle's privacy policies are convoluted, opaque, and not reasonably comprehensible to the average Internet user. Oracle's website leads to *seven* different privacy policies.[139] These privacy policies are sometimes complementary, sometimes exclusive, and always vague about how they relate to one another. For example, the "Oracle Advertising Privacy Policy," the "AddThis Privacy Policy," and the "Oracle General Privacy Policy" all provide different and non-uniform information about how the company uses cookies, leaving even an informed reader who seeks to educate themselves on how Oracle may be tracking and using their data confused as to what exactly Oracle is doing.[140]

110. Oracle's privacy policies fail to meaningfully disclose what Oracle does with internet users' information. Oracle's so-called privacy policies fail to meaningfully disclose that

[138] *See* Alessandro Acquisti, Curtis Taylor et al., *The Economics of Privacy*, 54 J. Econ. Literature 442 (2016), https://pubs.aeaweb.org/doi/pdfplus/10.1257/jel.54.2.442 [https://perma.cc/3KPV-5WHV]; Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (2018); Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital Resignation*, 21 new media & soc'y (2019), https://doi.org/10.1177/1461444819833331 [https://perma.cc/J8B4-K3ES].

[139] *See, e.g.*, *Privacy @ Oracle*, Oracle, https://www.oracle.com/legal/privacy/privacy-policy.html [https://perma.cc/V848-G7BS] (described as the "General Oracle Privacy Policy," but also referring to the "Services Privacy Policy" for " information on how Oracle processes services personal information.").

[140] *Oracle Advertising Privacy Policy*, Oracle (Last updated May 5, 2022), https://www.oracle.com/legal/privacy/advertising-privacy-policy.html [https://perma.cc/MP25-TAXY]; *AddThis Privacy Policy*, Oracle (Last updated May 5, 2022), https://www.oracle.com/legal/privacy/addthis-privacy-policy.html [https://perma.cc/E84S-W96V]; *Oracle General Privacy Policy*, Oracle (Last updated May 5, 2022), https://www.oracle.com/legal/privacy/privacy-policy.html [https://perma.cc/V848-G7BS].

Oracle's customers pay to use Oracle's ID Graph, Data Marketplace, and related services which Oracle promises will provide near-omniscience into the lives of Internet users.

111. The Oracle Advertising Privacy Policy understates the depth of Oracle's surveillance by failing to disclose its true range of categories of personal information that gives it visibility into people's lives. This particular policy exclusively uses an example of an internet user being targeted based on *one* characteristic: their interest in a Hawaiian vacation. Oracle's specific example is "age bracket 25-55; adventurous traveler; surfing enthusiast; in market for travel specials to Hawaii."[141] This sanitized illustration is impossible to square with the total visibility into Internet users' lives that Oracle provides to clients, and the reality that the segments Oracle offers regularly stretch to over a thousand categories.

112. Oracle is also conspicuously silent about the Data Marketplace in its disclosures. While the company touts the existence of "the world's largest third-party data marketplace" in client-facing marketing materials, its privacy policies *do not even mention the Data Marketplace's existence*. Although Oracle boasts elsewhere that the Data Marketplace hosts third parties who sell internet users' sensitive personal data,[142] Oracle's privacy policies fail to disclose that Oracle partners with other data brokers, nor provide the identity of these data broker partners.

113. The Oracle Advertising Privacy Policy states that Oracle classifies "political … orientation" as sensitive information, does not create "interest segments that reflect personal information that we consider sensitive," and has "operational procedures … to prevent our partners and customers from using personal information provided to them by Oracle to create interest segments that we consider sensitive."[143] Any reasonable reader would infer from this that Oracle does not facilitate the sale of their political views. In fact, the opposite is true: Oracle's

[141] *Oracle Advertising Privacy Policy*, Oracle (Last updated May 5, 2022), https://www.oracle.com/legal/privacy/advertising-privacy-policy.html[https://perma.cc/MP25-TAXY].

[142] *2019 Data Directory*, Oracle (2019), https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf [https://perma.cc/EV8L-PG7V].

[143] *Oracle Advertising Privacy Policy*, Oracle (Last updated May 5, 2022), https://www.oracle.com/legal/privacy/advertising-privacy-policy.html [https://perma.cc/MP25-TAXY].

advertising materials highlight the fact that data brokers on the Data Marketplace sell data on individuals' politics.[144]

114. In practice, the "notice and consent" framework that permeates the Internet is farcical. For example, a recent forensic investigation revealed that, in the context the IAB[145] Europe "Transparency Consent Framework" (TCF), even when users specifically decline consent to be tracked, various adtech participants—including Oracle—ignore those expressions of consent and place trackers on users' devices.[146] The same study discovered that Oracle places tracking cookies on a user's device *before the user even has a chance to decline consent*.[147] The IAB's CCPA Framework is broadly similar to the European TCF, and is directed at Internet users in California.[148]

115. Neither Oracle's so-called privacy policies, or the policies of third party Internet publishers, could provide any reasonable basis for Plaintiffs and Class members to have consented to Oracle's data collection, compiling of digital dossiers, and other data exploitation practices, or

[144] Oracle's professed decision to not selling political data is a recent development. As of 2016, its marketing materials prominently advertised its data on individuals' political views. *The Audience Playbook, Inspiration for winning campaigns*, Oracle (Aug. 2016), http://online.pubhtml5.com/mdhz/hgpp/#p=16 [https://perma.cc/4CUE-JKKV].

[145] The "Interactive Advertising Bureau (IAB) is an American advertising business organization that develops industry standards, conducts research, and provides legal support for the online advertising industry." Wikipedia, *Interactive Advertising Bureau*, https://en.wikipedia.org/wiki/Interactive_Advertising_Bureau [https://perma.cc/FP9B-VE7B].

[146] *Are Ad Tech Vendors in Europe Ignoring User Consent Signals?*, Adalytics, https://adalytics.io/blog/adtech-not-checking-user-tcf-consent [https://perma.cc/W2R6-SUMY] ("Pierre's TCF string shows that he only consented to basic ads (and only from Google). He is curious as to whether this ad creative that was served to his browser is indeed a "basic ad", devoid of any tracking or measurement pixels. He takes a look at the details of the "ad" attribute that was sent in the HTTPS response. The Balenciaga ad contains tracking and ad viewability or render pixels from TripleLift, Google, Oracle Moat, and The Trade Desk.")

[147] *Id.* ("[A]another EU citizen with a German IP address (we shall refer to them as "Charlotte"), creates a brand new Chrome instance, with no logins, cookies, local storage, or browser history. Charlotte proceeds to visit reuters.com. As soon as Charlotte opens the Reuters landing page, she is shown a cookie consent banner from OneTrust. *Before Charlotte has a chance to make any consent decisions or to read the consent text, several third party domains set cookies in Charlotte's browser*. We can observe Oracle Eloqua Marketing Automation ("eloqua.com") sets a cookie called "ELOQUA GUID", which Oracle's documentation says is a "global unique identifier" to help personalize websites.") (emphasis added).

[148] James Hercher, *The IAB Finalizes CCPA Framework As Industry Readies For More Regulators*, ad exchanger (Dec. 5, 2019, 1:04 PM), https://www.adexchanger.com/online-advertising/the-iab-finalizes-ccpa-framework-as-industry-readies-for-more-regulators/ [https://perma.cc/Q2CX-GLU4].

to have waived their privacy rights, including to be free from Oracle's pervasive surveillance of them.

116. Oracle knows, or reasonably should know, that Internet users such as Plaintiffs and Class members have insufficient knowledge or basis to reasonably comprehend the extent to which Oracle is obtaining their data, tracking their activity, and compiling it into digital dossiers, nor the deeply invasive and detailed nature of those dossiers. Oracle makes no disclosure anywhere directly to Plaintiffs or Class members of these practices. To the extent Plaintiffs or Class members indirectly acknowledge to third parties the presence of some aspect of an isolated data collection practice, or tracking cookie on an individual website, such acknowledgement in no way does or could reflect any consent or sufficient understanding of Oracle's practices.

117. As a data broker, Oracle effectuates ongoing, comprehensive surveillance of the Plaintiffs and Class members which grievously intrudes upon their privacy and which inevitably results in the corrosion of their individual autonomy and the collective autonomy of the society at large. Ordinary people, such as the Class members, do not and cannot possess an appropriate level of knowledge about the substantial threats that Oracle's surveillance poses to their own autonomy (in addition to lacking information sufficient to comprehend the nature and extent of Oracle's surveillance and its other implications). The social harms posed by Oracle's conduct impair not only individual autonomy, but the collective autonomy of Class members, as all members of a society have an interest in the enforcement of privacy rights, freedom from surveillance, and preservation of autonomy. Evisceration of these privacy values inexorably leads to the abrogation of the autonomy and freedom of the citizenry which are essential to the proper functioning of democratic republics. These harms caused by Oracle far outweigh the commercial benefits that extend to a private corporation. In the context of Oracle's practices, valid consent from Plaintiffs and the Class members is not only absent, it is not even possible.

118. Plaintiffs and Class members in fact have not waived their fundamental right to be free from the pervasive surveillance Oracle subjects them to. In any event, even were there any basis to conclude that Plaintiffs and Class members could be considered to have waived their

reasonable expectation of privacy with respect to Oracle's practices (and there is not), such waiver would be void and invalid as against public policy.

VII. CLASS ALLEGATIONS

119. Plaintiffs bring this class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes, which are jointly referred to throughout this Complaint as the "Classes:"

> United States Class:
>
> All natural persons located in the United States whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle's ID Graph or Data Marketplace.
>
> California Sub-Class:
>
> All natural persons located in California whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle's ID Graph or Data Marketplace.
>
> California Invasion of Privacy Act ("CIPA") Sub-Class:
>
> All members of the California Sub-Class whose contents of their electronic communications were intercepted by the use of Oracle's bk-coretag.js functionality.
>
> Florida Sub-Class:
>
> All natural persons located in Florida whose personal information, or data derived from their personal information, was used to create a profile and made available for sale or use through Oracle's ID Graph or Data Marketplace.
>
> Florida Security of Communications Act ("FSCA") Sub-Class:
>
> All members of the Florida Sub-Class whose contents of their electronic communications were intercepted by the use of Oracle's bk-coretag.js functionality.
>
> Electronic Communications Privacy Act ("ECPA") Sub-Class:
>
> All members of the United States Class whose contents of their electronic communications were intercepted by the use of Oracle's bk-coretag.js functionality.

120. Excluded from the Classes are the following individuals: officers and directors of Oracle and its parents, subsidiaries, affiliates, and any entity in which Oracle has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

121. Plaintiffs reserve the right to modify or amend the definition of each of the proposed Classes before the Court determines whether certification is appropriate.

122. This action readily satisfies the requirements set forth under Federal Rule of Civil Procedure 23:

a. Each Class is so numerous that joinder of all members is impracticable. Upon information and belief, Class members number in the millions.

b. There are questions of law or fact common to the Classes. These questions include, but are not limited to, the following:

1) Whether Oracle's acts and practices complained of herein amount to egregious breaches of social norms;

2) Whether Oracle acted intentionally in violating Plaintiffs' and Class members' privacy rights;

3) Whether Oracle was unjustly enriched as a result of its violations of Plaintiffs' and Class members' privacy rights;

4) Whether an injunction should issue; and

5) Whether declaratory relief should be granted.

c. Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs and the Class members did not consent to Oracle's interception, collection, analysis, and sale or their personal information, which acts form the basis for this suit.

d. Moreover, like all Class members, Plaintiffs suffer a substantial risk of repeated injury in the future. Each Plaintiff continues to use devices that are capable of reporting personal information to Oracle. Oracle's actions have thwarted and continue to threaten Plaintiffs' (and Class members') ability to exercise control over their own privacy while using their devices. Because the conduct complained of herein is systemic, Plaintiffs and all Class members face substantial risk of the same injury in the future. Oracle's conduct is common to all Class members and represents a common pattern of conduct resulting in injury to all members of the Classes. Plaintiffs have suffered the harm alleged and have no interests antagonistic to any other Class member.

e. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs' interests do not conflict with the interests of the Class members. Furthermore, Plaintiffs have retained competent counsel experienced in class action litigation, consumer protection litigation, and electronic privacy litigation. Plaintiffs' counsel will fairly and adequately protect and represent the interests of the Classes. Federal Rule of Civil Procedure 23(a)(4) and 23(g) are satisfied.

f. In acting as above-alleged, Oracle has acted on grounds generally applicable to the Classes, thereby making final injunctive relief and corresponding declaratory relief each appropriate with respect to the Classes as a whole. The prosecution of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Oracle.

VIII. <u>CAUSES OF ACTION</u>

<u>First Cause of Action</u>
Invasion of Privacy Under the California Constitution
(on behalf of the California Sub-Class)

123. Plaintiff Katz-Lacabe and the California Subclass members repeat and reallege all preceding paragraphs contained herein.

124. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted by California voters in 1972.

125. The phrase "and privacy" was added in 1972 after voters approved a proposed legislative constitutional amendment designated as Proposition 11. Proposition 11 was intended to curb businesses' control over the unauthorized collection and use of peoples' personal information, as the ballot argument stated:

> The right of privacy is the right to be left alone…It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control

> circulation of personal information. This is essential to social relationships and personal freedom.[149]

126. This amended constitutional provision addresses the concern over accelerating encroachment on personal freedom and security caused by increasing surveillance and data collection activity in contemporary society. Its proponents meant to afford individuals more measure of protection against this most modern threat to personal privacy:

> Computerization of records makes it possible to create ‘cradle-to-grave’ profiles of every American. At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian.[150]

In recognizing these privacy rights, the California Constitution provides insight into and serves to define the nature of the reasonable expectation of privacy of an objectively reasonable California resident. In contravention to the California Constitution and the reasonable expectations of privacy of California residents, Oracle “stockpil[es] unnecessary information about [Class members] and [] misus[es]information gathered for one purpose in order to serve other purposes,” creating “cradle-to-grave” profiles of Class members.

127. Plaintiff Katz-Lacabe and the California Subclass members maintain a reasonable expectation of privacy in the conduct of their lives, including their internet browsing activities and in their electronic communications and exchange of personal data. The reality of modern life increasingly requires that much of our daily activities are conducted online—Plaintiff Katz-Lacabe and the California Subclass members have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet. The necessary engagement with the digital world makes Plaintiff Katz-Lacabe’s and the California Subclass members’ private lives susceptible to unlawful observation and recording, capable of yielding a comprehensive and intrusive chronicle of Plaintiff Katz-Lacabe’s and the California Subclass members’ lives. If Plaintiff Katz-Lacabe and the California Subclass members do not have a reasonable expectation of privacy in the conduct of their lives online and the digital transmission of their personal data, they can have no reasonable expectation of privacy for virtually any facet of their lives.

[149] Ballot Pamp., Proposed Stats. & Amends. To Cal. Const. With Arguments to Voters. Gen. Election *26 (Nov. 7, 1972).

[150] *Id.*

128. Oracle, in violation of Plaintiff Katz-Lacabe's and the California Subclass members' reasonable expectation of privacy, intercepts, collects, tracks and compiles their web browsing activity and communications.

129. The nature and volume of the web browsing data collected is such that Oracle's practice of compiling dossiers based on the data it collects violates Plaintiff Katz-Lacabe's and the California Subclass members' reasonable expectation of privacy. Technological advances, such as Oracle's use of cookies, pixels, JavaScript, and other means to track and compile internet browsing activity, electronic purchases, and electronic communications, provide Oracle with the means to assemble a comprehensive chronicle of Plaintiff Katz-Lacabe's and the California Subclass members' lives heretofore unseen. Oracle collects and compiles personal information such as Plaintiff Katz-Lacabe's and the California Subclass members' email addresses, location data, and web browsing information, including that relating to race, religion, sexual orientation, and health. Such information is "personal information" under California law, which defines personal information as including "Internet or other electronic network activity information," such as "browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

130. Oracle also collects and analyzes Plaintiff Katz-Lacabe's and the California Subclass members' real-world offline activity, including activities like brick-and-mortar store purchases and location information, and compiles computerized records of those activities. Plaintiff Katz-Lacabe and the California Subclass members do not and cannot know which specific real-world offline activities Oracle may or may not be collecting and analyzing and adding to the digital dossiers it compiles on them.

131. Oracle's conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

a. Oracle engages in dragnet-style collection and interception of Plaintiff Katz-Lacabe's and the California Subclass members Internet activity, including their communications with websites, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.

b. Oracle also collects minute details about Plaintiff Katz-Lacabe's and the California Subclass members' *offline* activities, including their brick-and-mortar purchases and location information. By its very nature, Plaintiff Katz-Lacabe and the California Subclass members cannot be aware of or consent to this conduct.

c. Oracle creates dossiers based on this online and offline data, which constitute precisely the sort of "cradle-to-grave profiles" the right to privacy under the California Constitution was created to constrain.

132. Oracle's amassing of the electronic information reflecting all aspects of Plaintiff Katz-Lacabe's and the California Subclass members' lives into dossiers for future or present use is in and of itself a violation of Plaintiff Katz-Lacabe's and the California Subclass members' right to privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, those dossiers are and can be used to further invade Plaintiffs' privacy, by, inter alia, allowing third parties to learn intimate details of Plaintiff Katz-Lacabe's and the California Subclass members' lives, and target them for advertising, political, and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control dissemination and use of information about them. Additionally, as described above, the social harms posed by Oracle's conduct impair not only individual autonomy, but the collective autonomy of Class members, which autonomy is essential to the proper functioning of democratic republics.

133. Plaintiffs have been harmed by Oracle's indiscriminate collection and sale of their internet activity, their geolocation information, and their real world activities and purchases.

134. Privacy advocates have repeatedly decried Oracle's practices. Oracle's conduct described herein has been the subject of numerous legal complaints and lawsuits in Europe and the U.K. by privacy advocates.

135. Legislators have recognized the pernicious and privacy-invasive nature of Oracle's conduct as described herein. Senator Wyden, in urging the Consumer Financial Protection Bureau to take action against data brokers, stated that "[d]ata brokers are serving as shady middlemen to sell [consumers'] personal information without any legal protections" and that selling consumers' personal information "giving them no choice in the matter, is an egregious abuse of consumers'

privacy." Senators Warren and Wyden have also stated that "[d]ata brokers profit from the location data of millions of people, posing serious risks to Americans everywhere by selling their most private information." The FTC has also warned consumers about the "shadowy" "data broker ecosystem" where "companies have a profit motive to share data at an unprecedented scale and granularity," including a "staggering" amount of "highly personal information that people choose not to disclose even to family, friends, or colleagues."[151]

136. Oracle has violated Plaintiff Katz-Lacabe's and the California Subclass members' reasonable expectation of privacy via Oracle's review, analysis, dissemination, and subsequent uses of Plaintiffs' and Class members' private and other browsing activity through Oracle's Data Cloud, ID Graph and Data Marketplace.

137. Oracle's practices as alleged herein violate Plaintiff Katz-Lacabe's and the California Subclass members' reasonable expectation of privacy and are highly offensive to a reasonable person, and constitute an egregious breach of the social norms.

138. The right to privacy in California's constitution creates a right of action for California residents against private entities such as Oracle. Oracle lacks a legitimate business interest in stockpiling and compiling the personal information of Plaintiff Katz-Lacabe and the California Subclass members.

139. Plaintiff Katz-Lacabe and the California Subclass members have been damaged by Oracle's invasion of their privacy and are entitled to just compensation and injunctive relief.

Second Cause of Action
Intrusion Upon Seclusion Under California Common Law
(on behalf of the United States Class, or in the alternative on behalf of the California Sub-Class)

140. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

141. California common law on intrusion upon seclusion is applicable for all members of the United States Class.

[151] Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the law Against Illegal Use and Sharing of Highly Sensitive Data*, The Federal Trade Commission (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use [https://perma.cc/V6XT-85YX].

142. In the alternative, Plaintiffs allege intrusion upon seclusion under California law on behalf of the California Sub-Class.

143. Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

144. Plaintiffs and Class members maintain a reasonable expectation of privacy in the conduct of their lives, including their Internet browsing activities and in their electronic communications and exchange of personal data. The reality of modern life increasingly requires that much of our daily activities are conducted online—Plaintiffs and Class members have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet. The necessary engagement with the digital world makes Plaintiffs' and Class members' private lives susceptible to unlawful observation and recording that is capable of yielding an comprehensive and intrusive chronicle of Plaintiffs' and Class members' lives. If Plaintiffs and Class members do not have reasonable expectation of privacy in the conduct of their lives online and the digital transmission of their personal data, they can have no reasonable expectation of privacy for virtually any facet of their lives.

145. Oracle, in violation of Plaintiffs' and Class members' reasonable expectation of privacy, intercepts, collects, tracks, and compiles their web browsing activity and communications.

146. The nature and volume of the web browsing data collected is such that Oracle's practice of compiling dossiers based on the data it collects violates Plaintiffs' and Class members' reasonable expectation of privacy. Technological advances, such as Oracle's use of cookies, pixels, and other means to track and compile internet browsing activity, electronic purchases, and electronic communications, provide Oracle with the means to assemble a comprehensive chronicle of Plaintiffs' and Class members' lives heretofore unseen. Oracle collects and compiles personal information such as Plaintiffs' and Class members' email addresses, location data, and web browsing information, including that relating to race, religion, sexual orientation, and health. Such information is "personal information" under California law which defines personal information as including "Internet or other electronic network activity information," such as "browsing history,

search history, and information regarding a consumer's interaction with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

147. Oracle also collects and analyzes Plaintiffs' and Class members' real-world offline activity, including activities like brick-and-mortar store purchases and location information, and compiles computerized records of those activities. Plaintiffs and Class members do not and cannot know which specific real-world offline activities Oracle may or may not be collecting and analyzing and adding to the digital dossiers it compiles on them.

148. Oracle's conduct as described herein is highly offensive to a reasonable person and constitutes an egregious breach of social norms, specifically including the following:

a. Oracle engages in dragnet-style collection and interception of Plaintiffs' and Class members' Internet activity, including their communications with websites, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.

b. Oracle also collects minute details about Plaintiffs' and Class Members' *offline* activities, including their brick-and-mortar purchases and location information. By its very nature, Plaintiffs and Class members cannot be aware of or consent to this conduct.

c. Oracle creates dossiers based on this online and offline data, which constitute precisely the sort of "cradle-to-grave profiles" the right to privacy under the California Constitution was created to constrain.

149. Oracle's amassing of the electronic information reflecting all aspects of Plaintiffs' and Class Members' lives into dossiers for future or present use is in and of itself a violation of Plaintiffs' and Class Members' right to privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, those dossiers are and can be used to further invade Plaintiffs' and Class Members' privacy, by, inter alia, allowing third parties to learn intimate details of Plaintiffs' and Class Members' lives, and target them for advertising, political, and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control the dissemination and use of information about them. Additionally, as described above, the social harms posed by Oracle's conduct impair not only individual autonomy, but the

collective autonomy of Class members, which autonomy is essential to the proper functioning of democratic republics.

150. Privacy advocates have repeatedly decried Oracle's practices. Oracle's conduct described herein has been the subject of numerous legal complaints and lawsuits in Europe and the U.K. by privacy advocates. For example, at least until September 2020, Oracle tracked and compiled information on Internet users in the European Union and the United Kingdom using data derived from "third-parties," as described in detail above.[152] As noted in the press, Oracle's announcement that it would no longer make this functionality available in Europe and the U.K. came "just weeks after Oracle and rival data broker Salesforce were named in a class-action lawsuit in both the U.K. and the Netherlands that could result in the two companies having to pay up to $11.7 billion in fines under GDPR rules."[153] Oracle publicly described that lawsuit as a "shake-down"—yet it purported to cease certain of the practices complained of in that lawsuit only weeks after it was filed.[154]

151. Legislators have recognized the pernicious and privacy-invasive nature of Oracle's conduct as described herein. Senator Wyden, in urging the Consumer Financial Protection Bureau to take action against data brokers, stated that "[d]ata brokers are serving as shady middlemen to sell [consumers'] personal information without any legal protections" and that selling consumers' personal information and "giving them no choice in the matter, is an egregious abuse of consumers' privacy." Senators Warren and Wyden have also stated that "[d]ata brokers profit from the location data of millions of people, posing serious risks to Americans everywhere by selling their most private information." The FTC has also warned consumers about the "shadowy" "data broker ecosystem" where "companies have a profit motive to share data at an unprecedented

[152] Ronan Shields, *Oracle to Shutter Third-Party Data Services in Europe*, Adweek (Sept. 9, 2020), https://www.adweek.com/programmatic/oracle-to-shutter-third-party-data-services-in-europe/ [https://perma.cc/6VAK-2G5U].

[153] *Id.*

[154] Natasha Lomas, *Oracle and Salesforce Hit with GDPR Class Action Lawsuits Over Cookie Tracking Consent*, TechCrunch (Aug. 14, 2020), https://techcrunch.com/2020/08/14/oracle-and-salesforce-hit-with-gdpr-class-action-lawsuits-over-cookie-tracking-consent/ [https://perma.cc/79R7-SFU9].

scale and granularity," including a "staggering" amount of "highly personal information that people choose not to disclose even to family, friends, or colleagues."[155]

152. Oracle has violated Plaintiffs' and Class members' reasonable expectation of privacy via Oracle's review, analysis, dissemination and subsequent uses of Plaintiffs' and Class members' private and other browsing activity through Oracle's Data Cloud, ID Graph, and Data Marketplace.

153. Oracle's practices as alleged herein violate Plaintiffs' and Class members' reasonable expectation of privacy and are highly offensive to a reasonable person, and constitute an egregious breach of the social norms.

154. Oracle lacks a legitimate business interest in stockpiling and compiling the personal information of Plaintiffs and Class members.

155. Plaintiffs and Class members have been damaged by Oracle's invasion of their privacy and are entitled to just compensation and injunctive relief.

156. As a result of Oracle's actions, Plaintiffs and Class members seek injunctive relief, in the form of Oracle's cessation of tracking practices in violation of Plaintiffs and Class members' rights, and destruction of all personal data obtained in violation of Plaintiffs and Class members' rights.

157. As a result of Oracle's actions, Plaintiffs and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Oracle's actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Oracle from engaging in future misconduct.

158. Plaintiffs seek restitution for the unjust enrichment obtained by Oracle as a result of unlawfully collecting Plaintiffs' personal data. These intrusions are highly offensive to a reasonable person. Further, the extent of the intrusion cannot be fully known, as the nature of

[155] Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the law Against Illegal Use and Sharing of Highly Sensitive Data*, The Federal Trade Commission (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use [https://perma.cc/V6XT-85YX].

privacy invasion involves sharing Plaintiffs' and Class members' personal information with potentially countless third parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Oracle's conduct is the fact that Oracle's principal goal is and was to surreptitiously monitor Plaintiffs and Class members and to allow third-parties to do the same.

159. The threat posed by advancements in technology and the ability to create detailed dossiers therefrom was recognized half a century ago. *See* generally Arthur R. Miller, *The Assault on Privacy* 24–54 (1971). With monumental increases in technologies, Professor Miller's alarm 50 years ago about technology's assault on privacy has now taken on special urgency: precisely the concerns he warned of have come to fruition in Oracle's conduct. Through this lawsuit Plaintiff and Class members seek to vindicate their common law right against Oracle's ongoing assault on their privacy.

Third Cause of Action
Intrusion Upon Seclusion Under Florida Common Law
(in the alternative, on behalf of the Florida Class)

160. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

161. In the alternative, Plaintiffs allege that Florida law on intrusion upon seclusion is applicable for all members of the Florida Class.

162. Under Florida law, one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or her private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. *See* Restatement (Second) of Torts § 652B (Am. Law Inst. 1977).

163. Oracle's conduct electronically intrudes into Dr. Golbeck's home and computer by surveilling her internet browsing activity and communications with websites, as described above, which were conducted from the solitude of her own home and her computer. Dr. Golbeck has a reasonable expectation of privacy to be free from Oracle's pervasive surveillance of her in home. Florida courts recognize that that engaging in repeated surveillance of another person can constitute the tort intrusion upon seclusion. Oracle's conduct in systematically surveilling Dr. Golbeck in her home by surveilling her browsing on her computer is tantamount to erecting a

camera in her home as she browses the internet, in order to thereafter surveil and record her activities on a consistent basis.

164. Oracle's conduct is outrageous and intolerable in a civilized community. Systematic and ongoing surveillance is unacceptable under Florida law, and Oracle's comprehensive surveillance of Class members has been repeatedly singled out as unacceptable by legislators, the FTC, and others, as described above at paragraphs 148-151. The outrageousness of Oracle's conduct is compounded by Oracle's compiling of profiles of Florida Class members using information collected through systematic surveillance, and selling that information to unknown third parties for profit, as described above.

165. Dr. Golbeck and Class members maintain a reasonable expectation of privacy in the conduct of their lives, including their Internet browsing activities and in their electronic communications and exchange of personal data. The reality of modern life increasingly requires that much of our daily activities are conducted online—Dr. Golbeck and Class members have no practical choice or ability but to conduct their daily lives substantially in the digital world, connected to the Internet. The necessary engagement with the digital world makes Dr. Golbeck's and Class members' private lives susceptible to unlawful observation and recording that is capable of yielding a comprehensive and intrusive chronicle of Plaintiff's and Class members' lives. If Dr. Golbeck's and Class members do not have reasonable expectation of privacy in the conduct of their lives online and the digital transmission of their personal data, they can have no reasonable expectation of privacy for virtually any facet of their lives.

166. Oracle, in violation of Dr. Golbeck and Class members' reasonable expectation of privacy, intercepts, collects, tracks and compiles their web browsing activity and communications.

167. The nature and volume of the web browsing data collected is such that Oracle's practice of compiling dossiers based on the data it collects violates Dr. Golbeck and Class members' reasonable expectation of privacy. Technological advances, such as Oracle's use of cookies, pixels, and other means to track and compile internet browsing activity, electronic purchases, and electronic communications, provide Oracle with the means to assemble a comprehensive chronicle of Dr. Golbeck and Class members' lives heretofore unseen. Oracle

collects and compiles personal information such as Plaintiffs' and Class members' email addresses, location data, and web browsing information, including that relating to race, religion, sexual orientation, and health.

168. Oracle also collects and analyzes Dr. Golbeck and Class members' real-world offline activity, including activities like brick-and-mortar store purchases and location information, and compiles computerized records of those activities. Plaintiffs and Class members do not and cannot know which specific real-world offline activities Oracle may or may not be collecting and analyzing and adding to the digital dossiers it compiles on them.

169. Oracle's conduct as described herein is highly offensive to a reasonable person and constitutes, specifically including the following:

a. Oracle engages in dragnet-style collection and interception of Dr. Golbeck and Class members' Internet activity, including their communications with websites, thereby learning intimate details of their daily lives based on the massive amount of information collected about them.

b. Oracle also collects minute details about Dr. Golbeck's and Class Members' *offline* activities, including their brick-and-mortar purchases and location information. By its very nature, Plaintiffs and Class members cannot be aware of or consent to this conduct.

c. Oracle creates dossiers based on this online and offline data.

170. Oracle's amassing of the electronic information reflecting all aspects of Dr. Golbeck's and Class members' lives into dossiers for future or present use is in and of itself a violation of Dr. Golbeck's and Class members' right to privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, those dossiers are and can be used to further invade Dr. Golbeck's and Class members' privacy, by, inter alia, allowing third parties to learn intimate details of Plaintiffs' and Class members' lives, and target them for advertising, political, and other purposes, as described herein, thereby harming them through the abrogation of their autonomy and their ability to control the dissemination and use of information about them. Additionally, as described above, the social harms posed by Oracle's conduct impair not only individual autonomy,

but the collective autonomy of Class members, whose autonomy is essential to the proper functioning of democratic republics.

171. Dr. Golbeck's privacy interests have been harmed by Oracle's indiscriminate collection and sale of her internet activity, her geolocation information, and her real world activities and purchases.

172. Oracle has violated Dr. Golbeck's and Class members' reasonable expectation of privacy via Oracle's review, analysis, dissemination, and subsequent uses of Dr. Golbeck's and Class members' private and other browsing activity through Oracle's Data Cloud, ID Graph, and Data Marketplace.

173. Oracle lacks a legitimate business interest in stockpiling and compiling the personal information of Dr. Golbeck and Class members.

174. Dr. Golbeck and Class members have been damaged by Oracle's invasion of their privacy and are entitled to just compensation and injunctive relief.

175. As a result of Oracle's actions, Dr. Golbeck and Class members seek injunctive relief, in the form of Oracle's cessation of tracking practices in violation of Dr. Golbeck's and Class members' rights, and destruction of all personal data obtained in violation of Dr. Golbeck's and Class members' rights.

176. As a result of Oracle's actions, Dr. Golbeck's and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Defendants' actions—which were malicious, oppressive, willful— were calculated to injure Dr. Golbeck and made in conscious disregard Dr. Golbeck's rights. Punitive damages are warranted to deter Oracle from engaging in future misconduct.

177. Dr. Golbeck and Class members seek restitution for the unjust enrichment obtained by Defendants as a result of unlawfully collecting their personal data. These intrusions are highly offensive to a reasonable person. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Dr. Golbeck's and Class members' personal information with potentially countless third parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of

Oracle's conduct is the fact that Oracle's principal goal was to surreptitiously monitor Dr. Golbeck and Class members and to allow third parties to do the same.

Fourth Cause of Action
Violation of the California Invasion of Privacy Act
(on behalf of the CIPA Sub-Class)

178. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

179. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

180. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

Under either section of the CIPA, a defendant must show it had the consent of all parties to a communication.

181. Oracle utilizes a proprietary software device, referred to as "bk-coretag.js" JavaScript code, to "extract," or intercept, "user attributes," which include the contents of users' communications with websites, and secretly sends them to Oracle while the users are in the process of communicating with those websites. Oracle's technical documentation explains that bk-coretag.js JavaScript code deployed by Oracle collects "user attributes" "such as product views, purchase intent, [and] add-to-cart actions"[156] and other communications that users have with websites and simultaneously copies and sends those communications to Oracle.

[156] *Oracle Data Cloud Core Tag Implementation*, Oracle, https://docs.oracle.com/en/cloud/saas/

182. Oracle places the bk-coretag.js JavaScript code on Internet users' electronic devices when they browse a website that contains certain Oracle code. Oracle uses the bk-coretag.js JavaScript code to intercept the contents of Internet users' communications with websites as described at paragraphs 44-50 above. At all relevant times, Oracle's tracking and interceptions of Plaintiff Katz-Lacabe's and CIPA Sub-Class members' internet communications was without authorization and consent from Plaintiff Katz-Lacabe and CIPA Sub-Class members. The interception by Oracle in the aforementioned circumstances were unlawful and tortious.

183. The communications intercepted by Oracle include "contents" of electronic communications made from Plaintiffs Katz-Lacabe and ECPA Sub-Class members to websites other than those operated by Oracle in the form of:

a. the URLs being browsed by the Internet user as well as the referrer URL;

b. webpage title;

c. webpage keywords;

d. "product page visits"

e. "purchase intent" signals;

f. "add-to-cart actions"; and

g. data entered by the user into forms on the website.

184. The URLs being browsed by the Internet user as well as the referrer URL and data entered by the user into forms on the website constitute contents of communications. "Product page visits", "purchase intent" signals;" "add-to-cart actions"; and keywords also constitute contents of communications.[157] These actions communicate the user's intent to a website; for

data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/DataIngest/coretag_implementation.html [https://perma.cc/8XVU-8Z2F].

[157] Contrary to Oracle's arguments in its Motion to Dismiss Reply brief (*see* Dkt. No. 35 at 13), Plaintiffs did not and do not concede that information related to product page visits, add-to-cart actions, purchase intent signals, and webpage keywords are not "contents" of communications, contrary to Oracle's argument in its motion to dismiss briefing. Plaintiffs previously cited cases finding that keywords, add-to-cart actions and similar intent signals and interactions constitute contents of communications. *See* Motion to Dismiss Opposition (Dkt. No. 30) at 19, citing "*In re Google RTB Consumer Priv. Litig.*, 2022 WL 2165489, at *10 ("URL of the page [being visited]"; "referrer URL that caused navigation to the current page**"; "details about the content within the site or app"; and "list of keywords about [the] site or app" constituted "contents" of communications for ECPA purposes**); *Saleh*, 562 F. Supp. 3d at 518 ("**customer's**

example, adding a book to a cart on a website is functionally equivalent to calling a bookstore and asking to put that book on hold. There is no question that a wiretap of such a phone conversation would intercept the "contents" of a communication. Actions demonstrating purchase intent on websites are no different.

185. On information and belief, Oracle intercepted detailed URLs of webpages Plaintiff Katz-Lacabe viewed, including URLs revealing searches Plaintiff performed, the information Plaintiff entered into forms, including searches for specific content, and communications with websites related to purchases or intended purchases, including product page visits, purchase intent signals and add-to-cart actions. Examples of webpages that Plaintiff Katz-Lacabe interacted with for which the contents of his communications were intercepted by Oracle include, but are not limited, to those listed in paragraph 6 above.

186. Oracle's non-consensual tracking of Plaintiff Katz-Lacabe's and CIPA Sub-Class members' internet communications was designed to attempt to learn at least some meaning of the content in the URLs and other data interception. The URLs being browsed by the Internet user as well as the referrer URL and data entered by the user into forms on the website constitute contents of communications. "Product page visits", "purchase intent" signals;" "add-to-cart actions"; and keywords also constitute contents of communications. These actions communicate the user's intent to a website; for example, adding a book to a cart on a website is functionally equivalent to calling a bookstore and asking to put that book on hold. There is no question that a wiretap of such a phone conversation would intercept the "contents" of a communication. Actions demonstrating purchase intent on websites are no different.

187. On information and belief, Oracle intercepted detailed URLs of webpages Plaintiff Katz-Lacabe viewed, including URLs revealing searches performed and sensitive content viewed, information Plaintiff Katz-Lacabe entered into forms, including but not limited to searches for specific content, and communications with websites related to purchases or intended purchases, including product page visits, purchase intent signals and add-to-cart actions.

purchasing selections," "keystrokes," and "interactions with" defendants' website were contents of communications for ECPA purposes)." (emphasis added).

188. The following items constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA, and even if they do not, Oracle’s deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of “any other manner”:

a. The computer codes and programs Oracle used to track Plaintiffs Katz-Lacabe’s and Class members’ communications, including JavaScript;

b. Plaintiffs Katz-Lacabe’s and CIPA Sub-Class members’ browsers and mobile applications;

c. Plaintiffs Katz-Lacabe’s and CIPA Sub-Class members’ computing and mobile devices;

d. The computer codes and programs used by Oracle to effectuate its tracking and interception of the Plaintiffs Katz-Lacabe’s and CIPA Sub-Class members’; and

e. The plan Oracle carried out to effectuate its tracking and interception of Plaintiffs Katz-Lacabe’s and Class members’ communications.

189. Plaintiff Katz-Lacabe and CIPA Sub-Class members have suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their personally identifiable information.

190. Pursuant to California Penal Code § 637.2, Plaintiffs Katz-Lacabe and CIPA Sub-Class members have been injured by the violations of California Penal Code § 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

Fifth Cause of Action
Violation of the FSCA, Fla. Stat. Ann. § 934.03
(on behalf of the FSCA Class)

191. Plaintiff Dr. Golbeck and the FSCA Class members repeat and reallege all preceding paragraphs contained herein.

192. It is a violation of the FSCA to intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any electronic communication. Fla. Stat. Ann. § 934.03(1)(a).

193. Further, it is a violation to intentionally use, or endeavor to use, "the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection[.]" Fla. Stat. Ann. § 934.03(1)(d).

194. The FSCA defines "intercept" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Fla. Stat. Ann. § 934.02(3).

195. Under the FSCA, "contents" includes, but is not limited to, "any information concerning the substance, purport, or meaning of that communication." Fla. Stat. Ann. § 934.02(7).

196. The FSCA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, interstate, or foreign commerce…." Fla. Stat. Ann. § 934.02(12).

197. Oracle utilizes a proprietary software device, referred to as "bk-coretag.js" JavaScript code, to "extract," or intercept, "user attributes," which include the contents of users' communications with websites, and secretly sends them to Oracle while the users are in the process of communicating with those websites. Oracle's technical documentation explains that bk-coretag.js JavaScript code deployed by Oracle collects "user attributes" "such as product views, purchase intent, [and] add-to-cart actions"[158] and other communications that users have with websites and simultaneously copies and sends those communications to Oracle.

198. Oracle places the bk-coretag.js JavaScript code on Internet users' electronic devices when they browse a website that contains certain Oracle code. Oracle uses the bk-coretag.js JavaScript code to intercept the contents of Internet users' communications with websites as described at paragraphs 44–50 above. At all relevant times, Oracle's tracking and interceptions of

[158] *Oracle Data Cloud Core Tag Implementation*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/DataIngest/coretag_implementation.html [https://perma.cc/8XVU-8Z2F].

Plaintiff Golbeck and FSCA Class members' internet communications was without authorization and consent from Dr. Golbeck and FSCA Class members. The interception by Oracle in the aforementioned circumstances were unlawful and tortious.

199. The communications intercepted by Oracle include "contents" of electronic communications made from Dr. Golbeck and FSCA Class members to websites other than those operated by Oracle in the form of:

a. the URLs being browsed by the Internet user as well as the referrer URL;

b. webpage title;

c. webpage keywords;

d. "product page visits"

e. "purchase intent" signals;

f. "add-to-cart actions"; and

g. data entered by the user into forms on the website.

200. The URLs being browsed by the Internet user as well as the referrer URL and data entered by the user into forms on the website constitute contents of communications. "Product page visits" "purchase intent" signals," "add-to-cart actions" and keywords also constitute contents of communications. These actions communicate the user's intent to a website; for example, adding a book to a cart on a website is functionally equivalent to calling a bookstore and asking to put that book on hold. Actions demonstrating purchase intent on websites are "contents" of a communication.

201. On information and belief, Oracle intercepted detailed URLs of webpages Dr. Golbeck viewed, including URLs revealing searches Dr. Golbeck performed, the information Dr. Golbeck entered into forms, including searches for specific content, and communications with websites related to purchases or intended purchases, including product page visits, purchase intent signals and add-to-cart actions. Examples of webpages that Dr. Golbeck interacted with for which the contents of her communications were intercepted by Oracle include, but are not limited, to those listed in paragraphs 14 and 15 above.

202. Oracle's non-consensual tracking of Dr. Golbeck's and FSCA Class members' internet communications was designed to attempt to learn at least some meaning of the content in the URLs and other data interception.

203. The following items constitute "[e]lectronic, mechanical, or other device[s]":

a. The computer codes and programs Oracle used to track Dr. Golbeck and FSCA Class members' communications, including JavaScript;

b. Dr. Golbeck's and FSCA Class members' browsers and mobile applications;

c. Dr. Golbeck's and FSCA Class members' computing and mobile devices;

d. The computer codes and programs used by Oracle to effectuate its tracking and interception of the Plaintiffs Golbeck and FSCA Class members' communications; and

204. The equipment utilized by Oracle to intercept Dr. Golbeck's and the FSCA Class members' electronic communications constitute an apparatus, electronic, or other device under the FSCA as (1) it is not a telephone or telegraph equipment, or any component thereof; and/or (2) it was not furnished to Oracle by a provider of wire or electronic communication services. Fla. Stat. Ann. § 934.02(4). Software constitutes a "device" for purposes of applying wiretap statutes.

205. Oracle violated § 934.03(1)(a) of the FSCA by intentionally intercepting Dr. Golbeck and the FSCA Class members electronic communications.

206. Oracle intentionally intercepted Dr. Golbeck's and the FSCA Class members' electronic communications without their prior consent. Oracle used the contents of those communications as described at paragraphs 140-169 above.

207. As a result of Oracle's conduct, and pursuant to § 934.10 of the FSCA, Dr. Golbeck and the FSCA Class members were harmed and are each entitled to "liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher[.]" Fla Stat. Ann. § 934.10(b).

208. Dr. Golbeck and the FSCA Class members are also entitled to "reasonable attorney's fees and other litigation costs reasonably incurred." Fla Stat. Ann. § 934.10(d).

209. Dr. Golbeck and the FSCA Class members are also entitled to an injunction.

210. Dr. Golbeck and the FSCA Class members suffered loss by reason of these violations, including, but not limited to, violation of their rights to privacy.

Sixth Cause of Action
Violation of the Federal Wiretap Act, 18 U.S.C. § 2510, et. seq.
(on behalf of the ECPA Sub-Class)

211. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

212. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

213. The Wiretap Act protects both the sending and receipt of communications.

214. 18 U.S.C. § 2520(a) provides a private right of action to any person whose “wire, oral, or electronic communication is intercepted, disclosed, or intentionally used “in violation of the Wiretap Act.

215. As described above, Oracle intercepts Plaintiffs Katz-Lacabe’s and Golbeck’s and ECPA Sub-Class members’ communications with websites by placing tracking devices, namely the bk-coretag.js JavaScript code, on Plaintiffs Katz-Lacabe’s and Golbeck’s and ECPA Sub-Class members’ devices while they are browsing the Internet. This code transmits to Oracle the specific webpages and information about the webpages Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members’ are browsing, as well as the other data described herein, which Oracle uses to enrich the dossiers it compiles on Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members.

216. Oracle’s actions in intercepting and tracking user communications while they were browsing the internet was intentional. On information and belief, Oracle is aware that it is intercepting communications in these circumstances and has taken no remedial action.

217. Oracle’s interception of internet communications that Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members were sending and receiving was done contemporaneously with the sending and receipt of those communications.

218. The communications intercepted by Oracle include "contents" of electronic communications made from Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members to websites other than those operated by Oracle in the form of:

a. the URLs being browsed by the Internet user as well as the referrer URL;

b. webpage title;

c. webpage keywords;

d. "product page visits"

e. "purchase intent" signals;

f. "add-to-cart actions"; and

g. data entered by the user into forms on the website.

219. The URLs being browsed by the Internet user as well as the referrer URL and data entered by the user into forms on the website constitute contents of communications. "Product page visits", "purchase intent" signals;" "add-to-cart actions"; and keywords also constitute contents of communications. These actions communicate the user's intent to a website; for example, adding a book to a cart on a website is functionally equivalent to calling a bookstore and asking to put that book on hold. There is no question that a wiretap of such a phone conversation would intercept the "contents" of a communication. Actions demonstrating purchase intent on websites are no different.

220. On information and belief, Oracle intercepted detailed URLs of web pages Plaintiffs viewed, including URLs revealing searches Plaintiffs performed, the information Plaintiffs entered into forms, including searches for specific content, and communications with websites related to purchases or intended purchases, including product page visits, purchase intent signals and add-to-cart actions.

221. The transmission of data between Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members on the one hand and the websites on which Oracle tracked and intercepted their communications on the other, without authorization were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate

commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

222. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The computer codes and programs Oracle used to track Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Sub-Class members' communications, including JavaScript code;

b. Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Sub-Class members' browsers and mobile applications;

c. Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Sub-Class members' computing and mobile devices;

d. The computer codes and programs used by Oracle to effectuate its tracking and interception of the Plaintiffs' and Class members' communications; and

e. The plan Oracle carried out to effectuate its tracking and interception of the Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Sub-Class members' communications while browsing the internet.

223. Oracle, in its conduct alleged here, was not providing an "electronic communication service," as that term is defined in 18 U.S.C. § 2510(12) and is used elsewhere in the Wiretap Act. Oracle was not acting as an Internet Service Provider (ISP).

224. Oracle was not an authorized party to the communication because Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members were unaware of Oracle's interception of their communications with websites, and did not knowingly send any communication to Oracle. Oracle could not manufacture its own status as a party to Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Sub-Class members' communications with others by surreptitiously intercepting those communications.

225. As described above, the communications between Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members on the one hand, and websites on the other, were simultaneous to, but *separate* from, the channel through which Oracle acquired the contents of those communications.

226. The interception by Oracle in the aforementioned circumstances was performed for the secondary and independent purpose of committing tortious acts in violation of the law, specifically:

a. Violating the California Constitution's prohibition on the compiling of electronic dossiers, which dossiers are enriched by the contents of the communications intercepted by Oracle, as described herein;

b. Violating the tort of intrusion upon seclusion by using the contents of the intercepted communications to create detailed profiles on Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members, and then making those profiles available through Oracle's Data Cloud, ID Graph, and Data Marketplace, as described herein;

227. On information and belief, Oracle was aware that its conduct of profiling Class Members was tortious and intended to violate Class Members' privacy and other rights. Oracle CEO Larry Ellison, in describing Oracle's amassing of profiles on Class members, acknowledged that Oracle's conduct was potentially illegal and was "scaring the lawyers": "[Oracle's conduct] is a combination of real-time looking at all of their social activity, real-time looking at where they are, including, micro-locations – *this is scaring the lawyers who are shaking their heads and putting their hands over their eyes* – knowing how much time you spend in a specific aisle of a specific store and what is in that aisle of a store."[159]

228. Parties engaged in tortious conduct such as blackmail, theft of business secrets, or the misappropriation of a person's identity, primarily intend to "make money" through that conduct. The goal of making money through advertising revenue does not sanitize the intentional commission of a tort by Oracle. The mere existence of a lawful purpose alone does not "sanitize a[n interception] that was also made for an illegitimate purpose." *Sussman v. ABC*, 186 F.3d 1200, 1202 (9th Cir.1999), cert denied, 528 U.S. 1131 (2000). The 1) compiling of electronic dossiers, which dossiers are enriched by the contents of the communications intercepted by Oracle in violation of the California Constitution, and 2) use of the contents of the intercepted

[159] *See* TechEvents, *Openworld 2016 keynote by Larry Ellison: Complete, Integrated Cloud*, YouTube (Sept. 19, 2016), at 1:15:25-50, https://www.youtube.com/watch?v=WY5qhLwIqBA.

communications to create detailed profiles on Class members and then make those profiles available through Oracle's Data Cloud, ID Graph, and Data Marketplace, in violation the tort of intrusion upon seclusion, are illegitimate purposes under the ECPA.

229. Consent is not a defense where a "communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Subsequent disclosure of the contents of the intercepted conversations for the purpose of further invading the Plaintiffs' privacy is a tortious act that satisfies this exception to consent. In addition to having the intent of profiting from the sale of Plaintiffs' personal information, Oracle knowingly and intentionally invaded Plaintiffs' privacy through intercepting their communications, compiling those communications into dossiers for sale, and then sharing the contents of those communications with third parties. Any disputes as to Oracle's intent under the wiretapping statute are to be decided by the jury.

230. After intercepting the communications, Oracle then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

231. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs Katz-Lacabe and Golbeck and ECPA Sub-Class members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Oracle in the future, and a reasonable attorney's fees and other litigation costs reasonably incurred.

Seventh Cause of Action
Unjust Enrichment under California Common Law
(on behalf of the United States Class, or in the alternative on behalf of the California Sub-Class)

232. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

233. California common law on unjust enrichment is applicable for all members of the United States Class.

234. In the alternative, Plaintiffs allege unjust enrichment under California law on behalf of the California Sub-Class.

235. Oracle has wrongfully and unlawfully trafficked in the named Plaintiffs' and the Class members' personal information and other personal data without their consent for substantial profits.

236. Plaintiffs' and Class members' personal information and data have conferred an economic benefit on Oracle.

237. Oracle has been unjustly enriched at the expense of Plaintiffs and Class members, and the company has unjustly retained the benefits of its unlawful and wrongful conduct.

238. It would be inequitable and unjust for Oracle to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

239. Plaintiffs and Class members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Oracle obtained as a result of its unlawful and wrongful conduct.

240. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant. Oracle has been unjustly enriched by virtue of its violations of Plaintiffs' and United States Class members' legally protected rights to privacy as alleged herein, entitling Plaintiffs and United States Class members to restitution of Oracle's enrichment. "[T]he consecrated formula 'at the expense of another' can also mean 'in violation of the other's legally protected rights,' without the need to show that the claimant has suffered a loss." Restatement (Third) of Restitution § 1, cmt. a.

241. The elements for a claim of unjust enrichment are (1) receipt of a benefit and (2) unjust retention of the benefit at the expense of another. The doctrine applies where plaintiffs, while having no enforceable contract, nonetheless have conferred a benefit on defendant which defendant has knowingly accepted under circumstances that make it inequitable for the defendant to retain the benefit without paying for its value.

242. It is a longstanding principle of law embodied in the Restatement (Third) of Restitution and Unjust Enrichment (2011) that a person who is unjustly enriched at the expense of

another may be liable for the amount of the unjust enrichment even if the defendant's actions caused the plaintiff no corresponding loss. Where "a benefit has been received by the defendant but the plaintiff has not suffered a corresponding loss or, in some cases, any loss, but nevertheless the enrichment of the defendant would be unjust ... [t]he defendant may be under a duty to give to the plaintiff the amount by which [the defendant] has been enriched." Rest., Restitution, § 1, com. e.

243. The comments to the Restatement (Third) explicitly recognize that an independent claim for unjust enrichment may be predicated on a privacy tort. Restatement (Third) of Restitution and Unjust Enrichment § 44 cmt. b ("Profitable interference with other protected interests, such as the claimant's right of privacy, gives rise to a claim under § 44 if the benefit to the defendant is susceptible of measurement").

244. Moreover, the Restatement recognizes that in the context of a privacy violation, the claimant need not be in direct privity with the wrongdoer, and likewise, California law imposes no requirement of privity to make out an unjust enrichment claim. The Restatement comments provide the following illustrative example:

> 10. On going out of business, Local Pharmacy sells Customers' prescription records and accompanying medical information to National Chain. In connection with the sale, Local Pharmacy agrees not to inform Customers of the pending disclosure of their records; the object of this provision is to allow National Chain to communicate with Customers once their files have been transferred. Because it gives Customers no opportunity to object to the disclosure of confidential information, the transaction between Local Pharmacy and National Chain is both a violation of Customers' protected right of privacy in their prescription records and a deceptive marketing practice under local law. By the rule of this section, Customers have a claim against Local Pharmacy for the proceeds of the sale of their confidential information, *and a claim against National Chain for the additional profits it derived from the unlawful transaction*." *Id*. § 44 cmt. b, illus. 10 (emphasis added).

245. Because "[a] person is not permitted to profit by his own wrong," *id.* § 3, "[g]ains realized by misappropriation, or otherwise in violation of another's legally protected rights, must be given up to the person whose rights have been violated." *Id.* ch. 5, introductory note. These principles are deeply ingrained in California law. California courts have long recognized a

common law claim based on unjust enrichment. In determining the remedy for such claims, California courts apply principles found in the Restatement.

246. California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss. The public policy of California does not permit one to 'take advantage of his own wrong' regardless of whether the other party suffers actual damage. Where the defendant has been unjustly enriched but the plaintiff has not proven any monetary loss, the proper remedy is for the defendant to disgorge those ill-gotten gains. A defendant acting in conscious disregard of the rights of another should be required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Without this result, there would be an insufficient deterrent to improper conduct that is more profitable than lawful conduct. "Restitution requires full disgorgement of profit by a conscious wrongdoer, not just because of the moral judgment implicit in the rule of this section, but because any lesser liability would provide an inadequate incentive to lawful behavior." Restatement (Third) of Restitution and Unjust Enrichment § 3, cmt. b.

247. The unauthorized use of Plaintiffs' and United States Class members' information for profit entitles them to profits unjustly earned. That is so, moreover, regardless of whether Plaintiffs and United States Class members planned to sell their data or whether the individual's data is made less valuable, and regardless of whether Plaintiffs were in privity with Oracle.

248. Oracle has unjustly profited from disclosing users' browsing histories, internet activity, and real world activity to third parties without Plaintiffs' and United States Class members' knowledge or consent.

249. A portion—but not all—of the unjust enrichment Oracle obtained was through the use of Plaintiffs' and United States Class members' web browsing activities. In addition to data related to web browsing, Oracle collected and sold information regarding Plaintiffs' and United States Class members' physical movements through geolocation data, and Plaintiffs' and United States Class members' offline purchases and activities, including through credit cards and brick-and-mortar establishments. The combination of this data with Plaintiffs' and United States Class

members' web browsing and purchase activity constitutes an invasion of privacy. Moreover, the access Plaintiffs and United States Class members received to those websites does not defeat their unjust enrichment claim because:

a. As described in section VI.E. above, Plaintiffs were not aware of Oracle's conduct while browsing websites and did not and could not consent to that conduct. Had Plaintiffs known of Oracle's conduct, Plaintiffs would not have visited those websites or, if such visits were unavoidable, would have taken additional precautions to avoid being tracked and profiled by Oracle. Oracle's conduct with respect to tracking Plaintiffs' conduct on any particular website cannot be viewed in isolation—the aggregation, compilation, analysis, and sale of that extensive information about Plaintiffs' internet viewing habits violates Plaintiffs' California Constitutional and common law rights. Moreover, the fruits of Oracle's illegal wiretapping of Plaintiffs' communications with many websites, in violation of criminal statutes, also contributed to Oracle's enrichment. Oracle's enrichment through violation of criminal wiretapping statutes is inherently unjust.

b. Plaintiffs were not aware of and did not consent to the collection of their location data by Oracle, which is independent of their visit to any website. Oracle was unjustly enriched by the acquisition and sale of Plaintiffs' geolocation data.

c. Plaintiffs were not aware of and did not consent to the collection of their real-world activity, such as brick-and-mortar purchases, which is independent of their visit to any website. Oracle was unjustly enriched by the acquisition and sale of Plaintiffs' brick-and mortar-purchase data.

250. Plaintiffs did not provide authorization for the use of their personal information, nor did Oracle provide them with control over its use to produce revenue. This unauthorized use of their information for profit entitles Plaintiffs to profits unjustly earned.

251. Plaintiffs' aggregate browsing histories carry financial value. Oracle was unjustly enriched by aggregate Plaintiffs' personal and sensitive data into detailed dossiers that it makes available to third parties.

252. Oracle Advertising, the service which appears to administer the products at issue in this Complaint, had revenue in 2021 alone of approximately $2 billion. An unknown portion of this revenue was generated through the wrongful acquisition and sale of Class members' data, as described herein. The portion of Oracle's revenue attributable to Oracle's wrongful conduct described herein is susceptible of measurement and can be determined through discovery.

253. A 2019 study co-authored by Robert J. Shapiro and Siddartha Aneja, titled *Who Owns America's Personal Information and What is it Worth*?, calculated the value of Americans' personal information gathered and used by various data brokers as follows: $13.3 billion in 2016, $13.8 billion in 2017, and $14.8 billion in 2018.[160]

254. It would be unjust and inequitable to allow Oracle to profit from its violation of the Plaintiffs and United States Class members' Constitutional, common law, and statutory rights as described herein. Oracle's conduct in creating cradle-to-grave profiles of Plaintiffs and United States Class members is conduct that was specifically singled out for disapprobation by the voters of California in amending the California Constitution. Oracle's conduct is highly offensive to a reasonable person, and as such, regardless of whether Plaintiffs received anything of value from the websites they visited, Oracle's profiting from its collection and use of their data violates California public policy and goes well beyond acceptable social norms.

255. Oracle was aware of the benefit conferred by Plaintiffs. Oracle CEO Larry Ellison described in detail Oracle's plan to profit from its acquisition and use of Class members' data. *See* paragraph 210, supra. Indeed, Oracle's Data Marketplace is premised entirely on the sale of such data to third parties. Oracle acted in conscious disregard of the rights of Plaintiffs and United States Class members and should be required to disgorge all profit obtained therefrom to deter Oracle and others from committing the same unlawful actions again.

[160] Robert Shapiro and Siddhartha Aneja, *Who Owns Americans' Personal Information and What Is It Worth?*, Future Majority (April 2019), available at https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf. While Oracle was not included in this particular study, on information and belief the value of the information collected and used by Oracle is similar to if not larger than those of the data brokers described in the study.

Eighth Cause of Action
Unjust Enrichment under Florida Law (in the alternative on behalf of Florida Sub-Class)

256. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

257. Plaintiffs allege this claim for Unjust Enrichment under Florida Law in the alternative on behalf of the Florida Sub-Class.

258. There are three elements of an unjust enrichment claim under Florida law: first, the plaintiff has conferred a benefit on the defendant; second, the defendant voluntarily accepted and retained that benefit; and, finally, the circumstances are such that it would be inequitable for the defendants to retain the benefit without paying for it.

259. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of legally protected rights that enriched a defendant. Oracle has been unjustly enriched by virtue of its violations of Plaintiff Golbeck's and the Florida Class members' legally protected rights to privacy as alleged herein, entitling Plaintiff Golbeck and the Florida Class members to restitution of Oracle's enrichment.

260. Oracle has wrongfully and unlawfully trafficked in Plaintiff Golbeck's and the Florida Class members' personal information and other personal data without their consent for substantial profits.

261. Plaintiff Golbeck's and the Florida Class members' personal information and data have conferred an economic benefit on Oracle. Oracle voluntarily accepted and retained that benefit.

262. Oracle has been unjustly enriched at the expense of Plaintiff Golbeck and the Florida Class members, and the company has unjustly retained the benefits of its unlawful and wrongful conduct, as described above. Oracle has violated Dr. Golbeck's right to privacy as well as her rights under the ECPA and the Florida FSCA. It would be inequitable and unjust for Oracle to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

263. Dr. Golbeck and Florida Class members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits Oracle obtained as a result of its unlawful and wrongful conduct.

Ninth Cause of Action
Declaratory Judgment that Oracle Wrongfully Accessed, Collected, Stored, Disclosed, Sold, and Otherwise Improperly Used Plaintiffs' Private Data and Injunctive Relief (on behalf of all Classes)

264. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

265. The gravamen of this controversy lies in Oracle's collection, tracking, and analysis of Plaintiffs' and Class members' personal information and behavior, and building dossiers based on that information and providing that information to third parties. Plaintiffs and Class members never consented to, or were even aware of, Oracle's conduct described herein.

266. Oracle's misconduct has put Plaintiffs' and Class members' privacy and autonomy at risk, and violated their dignitary rights, privacy, and economic well-being.

267. Accordingly, Plaintiffs seek appropriate declaratory relief, and injunctive relief as prayed for below.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Issue an order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class representatives, that Plaintiffs' attorneys shall be appointed as Class counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

B. Certify this action is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

C. Appoint Plaintiffs to represent the Classes;

D. Appoint undersigned counsel to represent the Classes;

E. Enter Judgment in favor of Plaintiffs and the members of the Class against Oracle awarding damages, including punitive damage, and/or nominal damages, to Plaintiffs and the Class members, in an amount according to proof at trial, including interest thereon;

F. Enter Judgment in favor of Plaintiffs and the members of the Class against Oracle awarding unjust enrichment and/or restitution of Oracle’s ill-gotten gains, revenues, earnings, or profits that it derived, in whole or in part, from its unlawful collection and use of Class members’ personal data, in an amount according to proof at trial;

G. Enter Declaratory Judgment in favor of Plaintiffs and the members of the Class against Oracle pursuant to 28 U.S.C. § 2201, declaring that Oracle’s conduct is unlawful as alleged herein.

H. Permanently restrain Oracle, and its officers, agents, servants, employees and attorneys, from intercepting, tracking, collecting, or compiling the personal information of Class members as alleged herein;

I. Award Plaintiffs and the Class members their reasonable costs and expenses incurred in this action, including attorneys’ fees and expert fees; and

J. Grant Plaintiffs and the Class members further equitable, injunctive, declaratory, or other relief as the Court deems appropriate.

X. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: May 22, 2023

Respectfully Submitted,

/s/ Michael W. Sobol

Michael W. Sobol (SBN 194857)
msobol@lchb.com
David T. Rudolph (SBN 233457)
drudolph@lchb.com
Jallé H. Dafa (SBN 290637)
jdafa@lchb.com
Nabila Abdallah (SBN 347764)
nabdallah@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Attorneys for Plaintiffs and the Class